FACHHOCHSCHULE WÜRZBURG SCHWEINFURT
FACHBEREICH INFORMATIK UND WIRTSCHAFTSINFORMATIK

D I P L O M A R B E I T

Vorgelegt an der **Fachhochschule Würzburg-Schweinfurt**
im Fachbereich **Informatik und Wirtschaftsinformatik**
zum Abschluss eines Studiums
im **Studiengang Informatik**

Studienschwerpunkt: Medieninformatik

Thema: Toolunterstützte Zertifizierung auf Basis der Common Criteria

Angefertigt in Fa./Institut: Siemens CT IC CERT
Otto-Hahn-Ring 6, 81730 München

Prüfer: Herr Prof. Eberhard Grötsch

Abgabetermin: 20.07.2005

Eingereicht von
Michael Stumpf
aus
Würzburg
Würzburg, 22.02.2005

Kurzzusammenfassung

Common Criteria. Mit diesem Kriterienwerk und dem dazugehörigen Evaluationshandbuch können offiziell genehmigte Zertifizierungsstellen eine Evaluation auf Basis von Common Criteria objektiv durchführen. Durch die **Zertifizierung** wird gewährleistet, dass ein IT-Produkt ausreichend nach folgenden Sicherheitskriterien geschützt ist: Vertraulichkeit, Integrität und Verfügbarkeit.

Im Mai 1998 wurde nach mehrjähriger Arbeit die Version 2.0 der Common Criteria fertig gestellt und im April 1999 die Version 2.1 veröffentlicht. Kurz darauf wurde sie von der Internationalen Standardisierungsorganisation (ISO) technisch unverändert als **Internationaler Standard ISO/IEC 15408** veröffentlicht.

Ein wesentlicher Bestandteil von CC ist, dass **Schutzprofile / Protection Profiles (PP)** die Anforderungen an die Funktionalität und die Vertrauenswürdigkeit zusammenfassen und das Sicherheitskonzept beschreiben. Mit dem Schutzprofil wird eine Vergleichsgrundlage für alle Produkte, die nach demselben Schutzprofil bewertet wurden, geschaffen.

Das Evaluationsergebnis muss dann auf einer **Vertrauenswürdigkeitsstufe / Evaluation Assurance Level (EAL)** basieren. Die Ergebnisse von CC sind daher mit anderen CC Evaluationen vergleichbar.

Eine **Evaluation** ist der Vorgang, IT-Sicherheitsprodukte und –konzepte durch eine sachverständige Stelle zu prüfen und zu bewerten. Aus der Evaluierung eines PP ergeben sich Evaluationsergebnisse, die in Katalogen festgehalten werden. Als Ergebnis der Evaluation steht dann eine Aussage, die beschreibt bis zu welchem Grad man dem EVG vertrauen kann, die Anforderungen zu erfüllen. Im Falle einer erfolgreichen Evaluation erstellt dann die Zertifizierungsstelle einen Zertifizierungsreport, der letztendlich zum Zertifikat führt.

Ein in Java implementiertes Open Source Tool zur Vorbereitung und Unterstützung des Evaluationsprozesses ist die **CC Toolbox**.

Das Ergebnis des Einsatzes der CC Toolbox in dieser Diplomarbeit ist ein selbst erstelltes standardisiertes Protection Profile für den zukünftigen Siemens internen Gebrauch, das **Radio Commander PP**. Es soll allgemeingültig sein für eine Vielzahl von Siemens Systemen und nur noch jeweils angepasst werden müssen. Von anderen Schutzprofilen unterscheidet sich das Radio Commander PP dadurch, dass es Sicherheitsanforderungen für die Betrachtung von Gesamtsystemen und nicht für einzelne Komponenten formuliert. Das vorliegende Radio Commander PP genügt der Vertrauenswürdigkeitsstufe EAL-4. Das vollständige Radio Commander PP liegt im Anhang bei und stellt den praktischen Teil dieser Diplomarbeit dar.

Damit CC noch mehr Einsatz finden wird, sind die an der Erstellung von CC beteiligten Institutionen zurzeit mit der Entwicklung der neuen Version 3.0 beschäftigt. Die neue Version wird voraussichtlich zwischen Mai und Juli 2005 veröffentlicht werden.

Abstract

Common Criteria -With this collection of criteria and the included Common Evaluation Methodology officially approved Certification Authorities may objectively perform an evaluation on the basis of Common Criteria. By courtesy of the certification it is guaranteed that an IT-Product is adequately protected by following security criteria: confidentiality, integrity and availability.

In May 1998, after several years of work, the version 2.0 of the Common Criteria was finished and in April 1999 the version 2.1 was published. Not long after that CC was published by the International Organization for Standardization (ISO) without technical changes as International Standard ISO/IEC 15408.

An essential part of CC is that Protection Profiles (PP) unites the assumptions of the functionality and the trustworthiness and describes the security concept. With the Protection Profile a compare basis for all products of the same Protection Profile is created.

The evaluation result must base on an Evaluation Assurance Level (EAL). Therefore, the results of CC are comparable with other CC evaluations.

An Evaluation is a procedure for proving and estimating IT security products and –concepts by an expert institution. Resulting from the evaluation of a PP there are evaluation results, which have to be put down in catalogues. As a result of the evaluation stands the statement describing the trust to certain extends in the Target of Evaluation (TOE) to fulfil the assumptions. In case of a successful evaluation the certification institute creates a certification report finally leading to the certificate.

A Java-implemented Open Source Tool for the preparation and support of the evaluation process is called CC Toolbox.

The result of using the CC Toolbox in this diploma thesis is a self created and standardised Protection Profile for future internal use by Siemens, the so called Radio Commander PP. It is universally valid for a great variety of Siemens systems and has only to be configured for the actual system. Differing from other Protection Profiles the Radio Commander PP formulates Security Assumptions for the inspection of overall systems and not for single components. The present Radio Commander PP meets the requirements of EAL-4. The complete Radio Commander PP is enclosed in the appendix and represents the practical part of this diploma thesis.

That the CC will find more exertion the institutes that are involved in creating the CC are engaged in developing the new version 3.0 at this time. The new version will be expected to be published between May to June 2005.

Toolunterstützte Zertifizierung auf Basis der Common Criteria

1.	Die Zertifizierung von IT Produkten	1
2.	Grundlagen und Begriffserklärungen	3
2.1	Die Zertifizierungsstandards	3
2.1.1	TCSEC	5
2.1.2	ITSEC	6
2.1.3	Common Criteria	7
2.1.4	CEM	9
2.2	Die Evaluation	9
2.3	Die Sicherheitszusammenhänge	10
2.3.1	Die Bedrohungen	10
2.3.2	Die Sicherheitspolitiken	11
2.3.3	Die Sicherheitsannahmen	11
2.3.4	Die Sicherheitsziele	11
2.3.5	Die Sicherheitsanforderungen	11
2.3.6	Die konkreten Sicherheitsfunktionen	12
2.3.7	Zusammenfassung der Sicherheitszusammenhänge	12
2.4	Die gesetzlichen Grundlagen	14
3.	Der Inhalt der Common Criteria	15
3.1	Das Allgemeine Modell	16
3.1.1	Klasse	19
3.1.2	Familie	19
3.1.3	Komponente	19
3.1.4	Paket	20
3.1.5	Schutzprofil	21
3.1.6	Sicherheitsvorgaben	21
3.2	Evaluationsergebnisse und Anforderungen an die Evaluation	22
3.3	Die Funktionalen Klassen	24
3.3.1	Sicherheitsprotokollierung	27
3.3.2	Kommunikation	28
3.3.3	Kryptografische Unterstützung	28
3.3.4	Schutz der Benutzerdaten	29
3.3.5	Identifikation und Authentifizierung	31
3.3.6	Sicherheitsmanagement	31
3.3.7	Privatheit	32
3.3.8	Schutz der EVG Sicherheitsfunktionen	33

3.3.9 Betriebsmittelnutzung 35
3.3.10 EVG Zugriff 35
3.3.11 Vertrauenswürdiger Pfad/Kanal 36

3.4 Die Vertrauenswürdigkeitsklassen 37
3.4.1 Prüfung und Bewertung des Schutzprofils 39
3.4.2 Prüfung und Bewertung der Sicherheitsvorgaben 40
3.4.3 Konfigurationsmanagement 41
3.4.4 Auslieferung und Betrieb 41
3.4.5 Entwicklung 42
3.4.6 Handbücher 43
3.4.7 Lebenszyklus-Unterstützung 43
3.4.8 Testen 44
3.4.9 Schwachstellenbewertung 44
3.4.10 Erhaltung der Vertrauenswürdigkeit 45

4. Die Evaluation auf der Basis von Common Criteria 46

4.1 Die Vorbereitung 46
4.2 Der Evaluations- und Zertifizierungsprozess 48
4.3 Das Zertifizierungsschema DIN 45001 (BSI & CC) 49
4.4 Die EAL-Stufen 50
4.5 Die Kosten einer CC-Evaluierung 56

5. Ein Common Criteria Tool 57

5.1 Die CC Profiling Knowledge Base 57
5.2 Die CC Toolbox 60
5.3 Das Radio Commander PP 63
5.4 Fazit der CC Toolbox 67

6. Die Zukunft von Common Criteria 68

6.1 Die CC Version 3.0 68
6.2 Ziele und Chancen für CC 69

Abbildungsverzeichnis 71

Tabellenverzeichnis 71

Literaturverzeichnis 72

Abkürzungsverzeichnis 75

Anhang CC Toolbox Guide 77

Anhang Radio Commander PP 105

Zusammenfassung 160

Toolunterstützte Zertifizierung auf Basis der Common Criteria

1. Die Zertifizierung von IT Produkten

„Die Informationstechnik (IT) hat im Verlauf von nur vier Jahrzehnten eine wichtige, oft sogar lebenswichtige Rolle in fast allen Bereichen jeder organisierten Gesellschaft eingenommen. Als Folge hieraus wurde Sicherheit ein entscheidender Bestandteil der Informationstechnik.“ [16)]

Angriffe auf IT-Produkte sind längst keine Seltenheit mehr, wie die „Studie Hackerangriffe“ zeigt. Im Durchschnitt wurden 0,5 bis 5 ernsthafte Hackerattacken pro Monat und System ermittelt. „E-Commerce-Sites, zum Beispiel E-Shopping Angebote und Online-Kataloge, wurden dabei von den Angreifern favorisiert.“ [23)] Die Abteilung CT IC CERT der Firma Siemens erforscht und bekämpft seit Jahren Angriffe auf IT-Systeme. Der Mitarbeiter Sven Lehmberg prognostiziert für die Zukunft, „dass Hacker in Zukunft ihr Angriffspotential nicht mehr so sehr auf Standardprodukte (Betriebssysteme, Datenbanken) lenken, sondern Applikationen als neues Angriffsziel entdecken werden. Dies bedeutet, dass in Zukunft Produkt-Sicherheitsaudits systematisch durchgeführt werden müssen, um eine adäquate Produktsicherheit zu erzielen. Risikoanalysen, Bedrohungsanalysen, Use-Cases der Kunden und Betreiber und Checklisten auf Audit-Teamseite müssen dazu dienen, dass ein effizientes und effektives Überprüfen der Eindringsicherheit garantieren werden kann. Hierbei bietet Common Criteria durch sein standardisiertes Vorgehen eine gute Basis um die Produktsicherheit zu erhöhen.“

Wenn ein Hersteller eines IT-Produkts die Gefahr von Angriffen auf sein Produkt ernst genommen und daher Gegenmaßnahmen getroffen und implementiert hat, kann er sich sein Produkt zertifizieren lassen. Durch eine erfolgreiche Zertifizierung wird dem Käufer und Anwender mitgeteilt, dass er dem IT-Produkt vertrauen kann und sich nicht auf die für ihn kaum nachvollziehbaren Angaben des Herstellers verlassen muss. „Vielen Anwendern von IT fehlen Wissen, Fachkenntnis oder die nötigen Mittel, um beurteilen zu können, ob ihr Vertrauen in die Sicherheit ihres IT-Produkts oder Systems angemessen ist, und sie möchten sich auch nicht allein auf die Versicherungen des Entwicklers verlassen. Die Anwender können deshalb, um ihr Vertrauen in die Sicherheitsmaßnahmen zu erhöhen, eine Analyse der Sicherheit (d.h. eine Sicherheitsevaluation) des IT-Produkts oder Systems in Auftrag geben.“ [13)]

Eine Sicherheitsevaluation eines Produkts kann also den Grad des Vertrauens in ein Produkt anhand von analytischen und allgemeingültigen Kriterien belegen. Einige der größten Auftraggeber für IT-Produkte verlangen von ihren Herstellern, dass diese ihre Produkte zertifizieren lassen, um die geforderte Sicherheitsqualität einzuhalten. „In den USA werden seit Juli 2002 für den Einsatz von Produkten im Behördenbereich sowie des Militärs nur noch Produkte mit CC-Zertifikat beschafft; dies gilt sogar für Produkte, die typischerweise nicht unbedingt als IT-Sicherheitsprodukte bezeichnen werden, wie beispielsweise digitale Fotokopierer.“, so Dr. Markus Mackenbrock vom Bundesamt für Sicherheit in der Informationstechnik. Der Hersteller, der dann noch einen Auftrag

bekommen will, muss seine Produkte also zwingend evaluieren. Doch für diesen Evaluationsprozess muss es einheitliche Standards geben, damit man die daraus resultierenden Zertifikate vergleichen und so mögliche Auswahlentscheidungen erst objektiv treffen kann. Nach einer Phase von nationaler Standardisierung hat sich im letzten Jahrzehnt ein internationaler Standard etabliert, auf dessen Basis heutzutage Sicherheitszertifikate allgemeingültig vergeben werden können: Common Criteria.

Mit diesem Kriterienwerk und dem dazugehörigen Evaluationshandbuch können offiziell genehmigte Zertifizierungsstellen eine Evaluation auf Basis von Common Criteria objektiv durchführen. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Einhaltung dieses Standards verantwortlich und entscheidet, wer eine Zertifizierung auf Basis von Common Criteria durchführen darf.

Durch die Zertifizierung wird gewährleistet, dass ein IT-Produkt ausreichend nach folgenden Sicherheitskriterien geschützt ist:

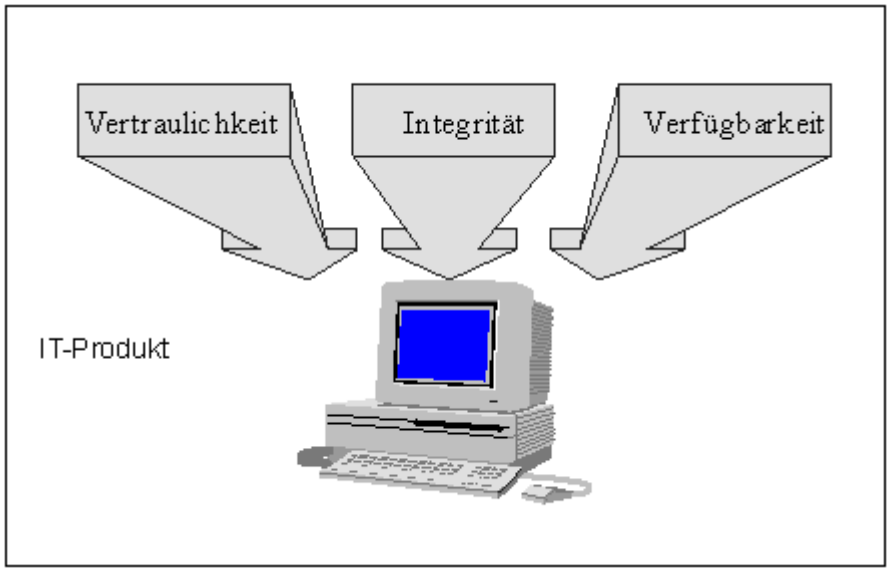


Abbildung 1

Vertraulichkeit: Schutz vor unbefugter Kenntnisnahme von Informationen.
Integrität: Schutz vor unbefugter Veränderung von Informationen.
Verfügbarkeit: Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln.

Diese Diplomarbeit wird im Folgenden verdeutlichen, was sich hinter dem Begriff Common Criteria versteckt, wie eine Evaluation nach Common Criteria abläuft und wie man den Zertifizierungsprozess durch die CC Toolbox unterstützen kann.

2. Grundlagen und Begriffserklärungen

Für das Verständnis des Evaluationsprozesses und der Zertifizierung ist es notwendig die folgenden Grundlagen zu kennen und die daraus resultierenden Zusammenhänge zu verstehen. Wer mit den Begriffen und Zusammenhängen vertraut ist und gleich tiefer in die Materie von Common Criteria einsteigen will, der kann das Kapitel zwei überspringen. Jedoch ist zu beachten, dass diese Arbeit auf den Grundlagen von Kapitel zwei aufbaut.

2.1 Die Zertifizierungsstandards

Die Schwierigkeit eines potentiellen Anwenders von IT-Produkten, ein vertrauenswürdiges System zu finden, das den aktuellen Sicherheitsstandards genügt, ist vor über 20 Jahren erkannt worden. In den USA beauftragte daraufhin im Jahre 1980 das US-Verteidigungsministeriums das National Computer Security Center der National Security Agency (NSA) einen Sicherheitskriterienkatalog zu erstellen. Die erste Version wurde Trusted Computer System Evaluation Criteria (TCSEC) genannt. Einige Jahre später wurden sie um die Trusted Network Interpretation zur Einbeziehung vernetzter Systeme erweitert. Bereits 1983 wurde TCSEC vom National Institute of Standards and Technology (NIST) herausgegeben. Aufgrund seines orangefarbenen Einbandes ist der Kriterienkatalog besser unter dem Namen "Orange Book" bekannt.

Eine Sicherheitszertifizierung der Produkte auf Basis von Sicherheitskriterien sollte eine Standardisierung herbeiführen, die als Richtschnur für die Entwicklung sicherer, vertrauenswürdiger Systeme und die objektive Bewertung dieser Systeme von einer neutralen und kompetenten Instanz (im Gegensatz zur Herstellererklärung) dienen kann. Dem Anwender ermöglicht dies ein geeignetes IT-Sicherheitsprodukt aufgrund dieser Zertifizierung auszuwählen. Da oftmals nicht IT-Spezialisten, sondern Manager die Entscheidung über die Auswahl eines Produktes treffen, hat eine Zertifizierung für den Entscheidungsträger eminente Bedeutung, um Produkte schneller nach Sicherheitskriterien vergleichen zu können, ohne sich erst den fachlichen Background aneignen zu müssen.

Im Jahre 1989 wurden als erstes nationales deutsches Kriterienwerk die IT-Sicherheitskriterien (ITS bzw. ITSK) veröffentlicht. Auch andere Länder, wie Großbritannien und Frankreich veröffentlichten ihre eigenen Kriterienkataloge. Aber schon zwei Jahre später im Jahre 1991 entstanden die Information Technology Security Evaluation Criteria (ITSEC) als gemeinsames Werk von Deutschland, Großbritannien, Frankreich und der Niederlande, um einen einheitlichen europäischen Standard zu schaffen. Dennoch existierte zu dieser Zeit noch kein gemeinsames international standardisiertes Kriterienwerk zwischen Europa und Nordamerika.

Dies sollte sich im Jahre 1996 ändern, als die Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik / Common Criteria for Information Technology Security Evaluation (CC) entstanden. Es folgte eine Überarbeitung der Kriterien bis zur Version 2.1 im Jahre 1999. Die Internationale Standardisierungsorganisation (ISO) hat CC als Internationalen Standard ISO/IEC

15408 veröffentlicht. Die CC basieren auf ihren Vorgängerwerken, gehen aber in ihrem Informationsgehalt und der Flexibilität darüber hinaus.

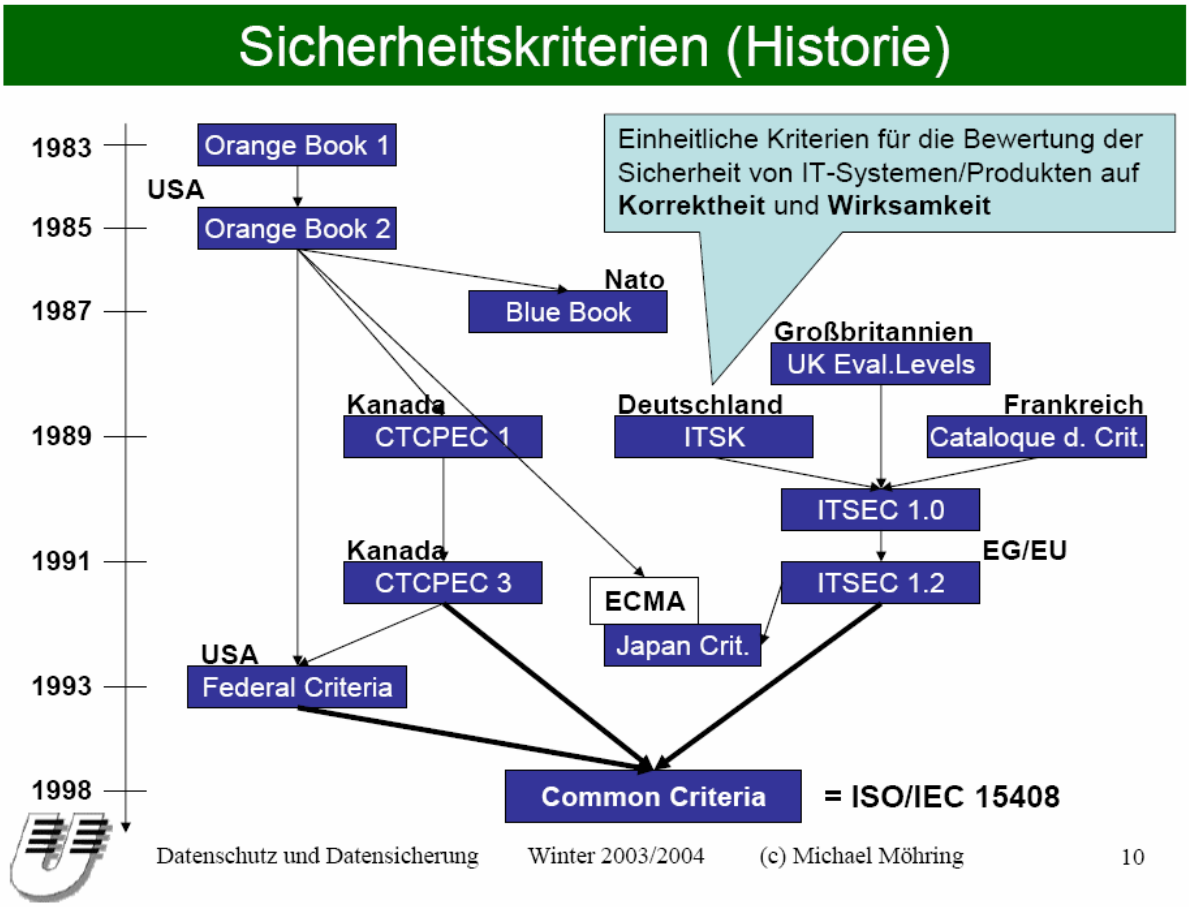


Abbildung 2

Um eine Zertifizierung nach CC durchzuführen, wurde 1999 die Common Evaluation Methodology (CEM) als Evaluationshandbuch veröffentlicht.

Bevor auf die einzelnen Standards genauer eingegangen wird, soll an dieser Stelle ein Vergleich von TCSEC, ITSEC und Common Criteria anhand der Vertrauenswürdigkeits- und Evaluationsstufen die gemeinsamen Beziehungen verdeutlichen und eine Vergleichsbasis der Evaluationsergebnisse dieser drei Standards schaffen. Eine genauere Erläuterung der EAL Stufen folgt später.

CC	TCSEC	ITSEC
---	D: Minimaler Schutz	E0
EAL-1	---	---
EAL-2	C1: Zugriffskontrolle auf Basis von Benutzerklassen	E1: informelle Beschreibung der Spezifikationen, einfache Tests
EAL-3	C2: Zugriffskontrolle auf Einzelbenutzerbasis	E2: detaillierte informelle Beschreibung der Spezifikationen, methodische Tests
EAL-4	B1: mindestens zwei explizite Sicherheitsklassen	E3: formales Sicherheitsmodell

EAL-5	B2: Sicherheitseinstufung umfasst gesamtes System; Login auf vertrauenswürdigem Weg	E4: zusätzlich zu E3 müssen Änderungen mitprotokolliert werden
EAL-6	B3: Sicherheitssystem erkennt Attacken; ist "widerstandsfähig" gegen Angriffe	E5: nachvollziehbare Abbildung zwischen Spezifikation und Quellcode
EAL-7	A1: formaler Nachweis der Sicherheit von Hard- und Software; verifizierte Sicherheit	E6: formale Entwurfsspezifikation; Konsistenz mit dem formalen Sicherheitsmodell ist nachzuweisen

Tabelle 1

2.1.1 TCSEC

Besser bekannt unter dem Namen „Orange-Book" sind die Trusted Computer System Evaluation Criteria (TCSEC) das erste Sicherheitskriterienwerk für IT-Produkte. Da das Werk im Auftrag des amerikanischen Verteidigungsministeriums entstand orientieren sich die Sicherheitskriterien stark an den Sicherheitsanforderungen militärischer Systeme und eignen sich daher nur eingeschränkt zur Beurteilung kommerzieller Systeme. Dennoch ist die Rolle von TCSEC nicht zu unterschätzen, da das amerikanische Justiz- und Verteidigungsministerium als einer der größten Auftraggeber von IT-Produkten von deren Herstellern die Zertifizierung nach TCSEC fordert.

Im Orange Book sind zum einen Sicherheitskriterien definiert und zum anderen Sicherheitsklassen, die stufenweise aufeinander aufbauen. Die Sicherheitskriterien sind in ihren jeweiligen Anforderungen an das System geordnet. Beginnend mit dem Kriterium 1 wird nur das Owner-Konzept verlangt, d.h., dass Ressourcen einem Eigner zugeordnet sind und dieser dann über eine weitere Vergabe bzw. den Entzug von Zugriffsrechten selbst entscheiden kann. Dagegen verlangt das Kriterium 6, dass das System formal spezifiziert und verifiziert ist.

Die Zertifizierung in Sicherheitsklassen baut auf den Sicherheitskriterien auf. Wenn ein System mit Sicherheitsklasse A zertifiziert ist, heißt dies, dass alle 6 Kriterien erfüllt sind; ein System, das mit Klasse C1 zertifiziert ist, braucht nur Kriterium 1 zu erfüllen. Ein System der Klasse D erfüllt keines der Kriterien. Die folgende Grafik verdeutlicht den Zusammenhang.

Das Orange Book

- Sicherheitskriterien
  1. Discretionary Access Control (DAC): Ressourcen sind einem Eigner zugeordnet; dieser kann über Vergabe und Entzug von Zugriffsrechten selbst entscheiden
  2. Identifikation von Benutzer-Aktionen durch LOGIN-Prozeduren und Beobachten sicherheitsrelevanter Ereignisse
  3. Mandatory Access Control (MAC): Einteilung von Objekten in Sicherheitsklassen; Zuordnung von Klassenrechten zu Benutzern, Referenz-Monitor zum Überwachen der Rechte
  4. Klar definiertes und dokumentiertes Sicherheitspolitik-Modell mit MAC; Kennzeichnung von Geräten; spezielle Authentifizierungsmechanismen
  5. Alle Benutzerzugriffe auf Ressourcen laufen über das System; Unterscheidung von Modulen nach Sicherheitsrelevanz; Sicherheitsbeauftragter existiert
  6. System ist formal spezifiziert und verifiziert
- Sicherheitsklassen

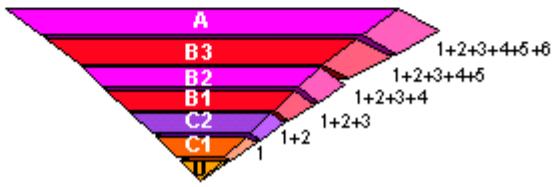


Abbildung 3

„Jede Kriterienklasse umfasst vier Aspekte der Evaluation: Sicherheitspolitik, Beweissicherung, Vertrauenswürdigkeit und Dokumentation. Die Kriterien für diese vier Aspekte werden von Klasse zu Klasse detaillierter und bilden eine Hierarchie, in welcher D die niedrigste und A1 die höchste Klasse darstellt. Jede dieser Klassen beinhaltet sowohl Forderungen an die Funktionalität als auch an die Vertrauenswürdigkeit.“ [16)]

Durch diese Einteilung in Sicherheitsklassen ist erstmals ein Vergleich zwischen zertifizierten IT-Produkten möglich geworden, der zumindest in den USA als Standard gültig war.

2.1.2 ITSEC

Im Jahre 1991 entstanden die Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik/Information Technology Security Evaluation Criteria (ITSEC) als gemeinsames Werk von Deutschland, Großbritannien, Frankreich und den Niederlanden, um einen einheitlichen europäischen Standard für die Zertifizierung von IT-Produkten zu schaffen. Es ist das europäische Gegenstück zu TCSEC und vereint die nationalen IT-Sicherheitskriterien.

„Während TCSEC einen klaren Fokus auf die Vertrauenswürdigkeit legt, ergänzt ITSEC die Betrachtungsweise um die Funktionalität. Zudem differenziert ITSEC bei der Vertrauenswürdigkeit zwischen Korrektheit und Wirksamkeit. Bei der Evaluierung kommerzieller Software ist ITSEC daher im Vorteil.“ [4)]

ITSEC legt sieben Evaluationsstufen fest, die das zunehmende Vertrauen in die Fähigkeit eines Evaluationsgegenstandes (EVG) widerspiegeln, seine Sicherheitsvorgaben zu erfüllen. Die Sicherheit eines EVG wird durch eine Kombination von Vertraulichkeit, Integrität und Verfügbarkeit beschrieben. Um diese Sicherheit zu

erreichen, müssen zuerst die Sicherheitsmaßnahmen auf den folgenden drei Ebenen beschrieben werden: Sicherheitsziele, sicherheitsspezifische Funktionen und Sicherheitsmechanismen. Da diese Begriffe auch in die Common Criteria übernommen wurden, folgt eine Erklärung erst im Anschluss. Durch die Einordnung eines Produktes in eine der sieben Evaluationsstufen wird genauso wie bei TCSEC eine Vergleichbarkeit zwischen verschiedenen IT-Produkten erreicht.

„Es ist jedoch nicht möglich, die Evaluationsstufen direkt mit den Vertrauensstufen der TCSEC-Klassen zu vergleichen, weil die Stufen der ITSEC im Rahmen einer Harmonisierung von mehreren europäischen IT-Sicherheitskriterienkatalogen entwickelt wurden und in diesen Katalogen etliche Anforderungen enthalten sind, die in den TCSEC nicht explizit erscheinen." [16)]

2.1.3 Common Criteria

Der offizielle Name der Common Criteria lautet „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik / Common Criteria for Information Technology Security Evaluation (CC)" [1)].

Im Mai 1998 wurde nach mehrjähriger Arbeit die Version 2.0 der Common Criteria fertig gestellt und im April 1999 die Version 2.1 veröffentlicht. Kurz darauf wurde sie von der Internationalen Standardisierungsorganisation (ISO) technisch unverändert als Internationaler Standard ISO/IEC 15408 veröffentlicht. Durch diesen Schritt hat sich CC als einheitlicher Standard etabliert, da CC für die Bewertung der Sicherheitseigenschaften praktisch aller informationstechnischen Produkte und Systeme geeignet ist. Die deutsche Übersetzung wurde am 29.09.2000 im Bundesanzeiger offiziell bekannt gegeben. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Ausstellung von Sicherheitszertifikaten auf der Basis der CC zuständig. Die jeweils aktuelle deutsche und englische Version der CC kann auf der offiziellen Homepage des BSI gelesen werden.

Die Erstellung der CC war ein internationales Projekt, an dem sich Deutschland, Frankreich, Großbritannien, Kanada, die Niederlande und die USA beteiligt haben. Daher wurde auch aus nationalen Interessen darauf geachtet, dass die schon bestehenden Zertifizierungsstandards aus diesen Ländern ITSEC, TCSEC und CTCPEC kompatibel zu den Basiskriterien der CC sind. In Deutschland bedeutet dies, dass alle Zertifikate auf Basis der ITSEC auch nach Einführung der CC vergleichbare Evaluationsergebnisse zu CC besitzen. Allerdings sind der Informationsgehalt und die Flexibilität der CC deutlich höher als bei den Vorgängerstandards.

„Damit verlieren die Zertifikate nationaler Organisationen zunehmend zu Gunsten der international anerkannten Common Criteria an Bedeutung. Zwar sind unabhängige Zertifikate wie die Common Criteria kein Allheilmittel, bieten Anwendern aber wichtige Entscheidungskriterien bei der Auswahl von Produkten." [4)]

Die CC gehen in Bezug auf die Anforderungen an die Vertrauenswürdigkeit und die Funktionalität eines Evaluationsgegenstandes über die bestehenden Zertifizierungs-standards hinaus.

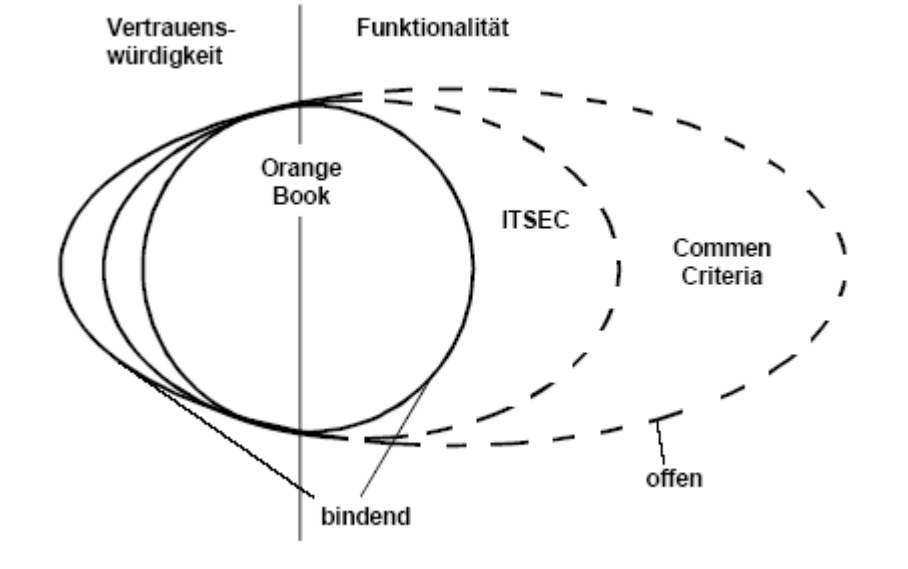


Abbildung 4

Ein wesentlicher Bestandteil von CC ist, dass Schutzprofile / Protection Profiles (PP) die Anforderungen an die Funktionalität und die Vertrauenswürdigkeit zusammenfassen und das Sicherheitskonzept beschreiben. Außerdem werden darin die Bedrohungen den Anforderungen gegenübergestellt. Die aufgestellten Schutzprofile können sogar bei der ISO registriert werden, um sicherzustellen, dass sie der gesamten interessierten Öffentlichkeit zur Nutzung offen stehen. Dadurch wird eine einheitliche Handhabung der CC gefördert.

Bei der folgenden Evaluation der Schutzprofile und des EVG wird dann überprüft, „ ... ob das Schutzprofil eine vollständige und in sich geschlossene Menge von Anforderungen ist und dass ein zu diesem Schutzprofil konformer EVG eine wirksame Menge von IT-Sicherheitsgegenmaßnahmen in der Sicherheitsumgebung bereitstellt.“ [1)]

Das Evaluationsergebnis muss dann auf einer Vertrauenswürdigkeitsstufe / Evaluation Assurance Level (EAL) basieren und dabei eventuell um weitere Anforderungen ergänzt werden. Es gibt dabei sieben hierarchische EAL Stufen in CC, wobei die niedrigste EAL Stufe nur einen funktionalen Test verlangt und die höchste EAL Stufe einen semiformalen verifizierten und getesteten Entwurf voraussetzt. Die genaue Abstufung wird im Kapitel „Die EAL Stufen“ dargelegt. Die Ergebnisse von CC sind daher mit anderen CC Evaluationen vergleichbar.

Die CC sind kein rein theoretisches Werk, sondern offensichtlich aus der praktischen Notwendigkeit entstanden. Die Praxisnähe zeigt sich darin, dass CC einen umfangreichen Katalog von Funktionalitätsanforderungen beinhaltet, der Beschreibungen für die Funktionalität eines IT-Produkts vorschlägt und so die Aufstellung der Schutzprofile erleichtert. Um auf der Basis von CC einheitlich zu evaluieren, wurde es nötig ein Evaluationshandbuch zu erstellen, die so genannte CEM.

2.1.4 CEM

Im Jahre 1997 wurde die erste Fassung der Gemeinsamen Evaluationsmethodologie/ Common Evaluation Methodology (CEM) veröffentlicht, die man als Evaluationshandbuch für CC bezeichnen kann. Dabei beschreibt CC was evaluiert und die Methodologie wie evaluiert werden soll.

„Ziel der internationalen Harmonisierung von IT-Sicherheitskriterien ist die formale gegenseitige Anerkennung von Evaluationsergebnissen. Wenn sichergestellt ist, daß von den beteiligten Stellen dieselben Kriterien und dasselbe Evaluationsverfahren in gleicher Weise angewendet werden, ist es erlaubt, ausreichendes Vertrauen in die Evaluationsergebnisse anderer Stellen zu haben. Als technische Grundlage dient hierzu die Erarbeitung einer gemeinsamen Evaluationsmethodologie (Common Evaluation Methodology, CEM) auf der Basis gemeinsamer IT-Sicherheitskriterien (Common Criteria, CC)." [10)]

An der Entwicklung der CEM sind dieselben Nationen und Organisationen beteiligt wie an CC. Dafür ist eine internationale Arbeitsgruppe, das Common Evaluation Methodology Editorial Board (CEMEB), gebildet worden, die sich regelmäßig in den beteiligten Ländern zur Entwicklung und Fortschreibung der CEM trifft.

2.2 Die Evaluation

Eine Evaluation ist der Vorgang, IT-Sicherheitsprodukte und –konzepte durch eine sachverständige Stelle zu prüfen und zu bewerten. Normalerweise werden die Evaluationsergebnisse dann durch eine Zertifizierungsstelle bestätigt. Die Durchführung der Evaluation erfolgt im Allgemeinen auf der Basis von Evaluationskriterien wie ITSEC oder CC. Der Evaluationsprozess kann in generischer Form in einem so genannten Evaluationshandbuch beschrieben werden. Beispiele hierfür sind die Information Technology Security Evaluation Methodology (ITSEM) und die CEM.

An einer Evaluation sind mehrere Stellen beteiligt, die unterschiedliche Aufgaben im Evaluationsprozess wahrnehmen:

- Der **Hersteller / Importeur** stellt den EVG und liefert die Evaluierungsdokumentation.

- Die **Prüfstelle** prüft die Evaluierungsdokumentation und den EVG, erstellt Prüfberichte und fertigt den Zertifizierungsreport.

- Die **Zertifizierungsstelle** prüft die Prüfberichte und den Zertifizierungsreport und vergibt dann ein Zertifikat.

Außerdem müssen vor einer Evaluation Vorgaben gemacht werden, damit klar ist, was die Evaluation prüfen soll. Diese werden in einer Spezifikation festgehalten. Dabei wird der Inhalt der Spezifikation aber weitgehend vom Hersteller des Produktes bestimmt. Das Ergebnis der Spezifikation sind Sicherheitsvorgaben für das IT-Produkt.

Wie eine Sicherheitsevaluierung auf Basis von CC ablaufen kann wird im Kapitel „Die Evaluation auf der Basis von Common Criteria“ beschrieben.

Die Evaluation ist also eine Möglichkeit, verlässliche Aussagen hinsichtlich der Sicherheitseigenschaften von IT-Produkten mittels deren Prüfung und Bewertung nach einheitlichen Kriterien durch unabhängige Stellen zu schaffen. Als Ergebnis der Evaluation kann dann ein Zertifikat über eine geprüfte Sicherheitsleistung stehen.

2.3 Die Sicherheitszusammenhänge

Um eine Spezifikation für eine Evaluation aufzustellen, müssen zuerst die Zusammenhänge zwischen den möglichen Bedrohungen für ein IT-Produkt und den entgegenwirkenden Sicherheitsmaßnahmen geklärt werden, damit am Ende dieses Klärungsprozesses konkrete Sicherheitsfunktionen für das Produkt festgehalten werden können. Die Zusammenhänge zwischen Bedrohungen, Sicherheitszielen, Sicherheitsanforderungen und Sicherheitsfunktionen werden im Folgenden betrachtet.

„Aus den Sicherheitszielen werden Sicherheitsanforderungen bestimmt, die der EVG durch seine Sicherheitsfunktionen erfüllt. Die sich daraus ergebenden Verknüpfungen zwischen den Bedrohungen und den Sicherheitsfunktionen bilden eine wechselseitige Abhängigkeit, aus der hervorgeht, dass zu jeder Bedrohung mindestens eine Sicherheitsfunktion existiert und zu jeder Sicherheitsfunktion mindestens eine Bedrohung zugehörig ist. Allgemein kann gesagt werden, dass der EVG Sicherheitsfunktionen bereitstellt, um sich vor Bedrohungen zu schützen.“ [12)]

Zum Verständnis der folgenden Begriffe kann es eventuell sinnvoll sein zwischendurch die Abbildung 5 im Kapitel „2.3.7 Zusammenfassung der Sicherheitszusammenhänge“ zu betrachten.

2.3.1 Die Bedrohungen

Die Bedrohungen stehen an der Spitze des oben genannten Zusammenhanges und richten sich gegen die zu schützenden Werte des EVG. Sie gilt es zuallererst zu identifizieren. Dafür wird für jeden zu schützenden Wert geprüft, ob und wie weit der Verlust der Verfügbarkeit, der Vertraulichkeit und der Integrität eine Bedrohung für den EVG darstellt. Um diesen Bedrohungen entgegenzuwirken, müssen Sicherheitsfunktionen definiert werden.

Allerdings gibt es auch Bedrohungen, die sich nicht direkt gegen den EVG richten, sondern seine Umgebung betreffen und denen nicht mittels Sicherheitsfunktionen entgegengewirkt werden kann. Beispielsweise kann der EVG nicht ordnungsgemäß in Betrieb genommen werden. Dagegen können keine Sicherheitsfunktionen für den EVG festgelegt werden.

2.3.2 Die Sicherheitspolitiken

Die organisatorischen Sicherheitspolitiken sind eine oder mehrere organisatorische Regelungen, Verfahren, Praktiken oder Richtlinien, denen der EVG entsprechen muss. In so genannten Sicherheitszielen wird analysiert, ob sich der EVG mit den Sicherheitspolitiken und allen identifizierten Bedrohungen verträgt. Der sich daraus ergebende Sicherheitsbedarf wird dann mit Hilfe von Sicherheitsfunktionen erfüllt.

2.3.3 Die Sicherheitsannahmen

Die Sicherheitsannahmen sind Annahmen über vorhandene Sicherheitsaspekte der EVG Umgebung. Sie beeinflussen die Sicherheitsziele des EVG. Eine mögliche Annahme wäre zum Beispiel die sichere Vernetzung des EVG. Daraus würde sich ergeben, dass die Vernetzung dann als sicher vorausgesetzt und nicht weiter betrachtet wird.

„Ferner können das Betriebsziel und der Produktzweck sowie mögliche Einschränkungen der Benutzung oder allgemein, Informationen über die Umgebung des EVG als Annahmen festgeschrieben werden. Genau wie die Bedrohungen führen auch die Annahmen über die Sicherheitsziele zu Sicherheitsanforderungen. Diese werden aber bei der Untersuchung der produktspezifischen Sicherheitsfunktionen nicht betrachtet, da die Sicherheitsannahmen Zustände darstellen, für die keine Sicherheitsfunktionen des EVG beschrieben werden können.“ [12)]

2.3.4 Die Sicherheitsziele

Die Sicherheitsziele werden definiert, um alle Zweifel an der Sicherheit und die Ziele der Sicherheitsaspekte zu berücksichtigen. Die Sicherheitsaspekte können den EVG oder seine Umgebung als Ziel haben. Mittels der Sicherheitsziele wird die Absicht erklärt, alle bekannten Bedrohungen zu vermeiden und organisatorische Sicherheitspolitiken sowie Sicherheitsannahmen zu erfüllen. Nichttechnische und organisatorische Mittel sind dabei für Sicherheitsziele der EVG Umgebung geeignet, während sich für Sicherheitsziele, die den EVG direkt betreffen, Sicherheitsanforderungen ableiten lassen.

2.3.5 Die Sicherheitsanforderungen

Die Sicherheitsanforderungen sollen sicherstellen, dass die Sicherheitsziele durch den EVG erfüllbar sind. Dabei werden die Sicherheitsanforderungen in funktionale Anforderungen und Anforderungen an die Vertrauenswürdigkeit unterschieden. Die funktionalen Anforderungen stellen Anforderungen an den EVG dar, wohingegen die Anforderungen an die Vertrauenswürdigkeit zusätzlich Kriterien für die Tiefe der Prüfung und der Bewertung berücksichtigen.

2.3.6 Die konkreten Sicherheitsfunktionen

Durch die konkreten Sicherheitsfunktionen erfüllt der EVG seine funktionalen Sicherheitsanforderungen, indem jede funktionale Sicherheitsanforderung mindestens eine konkrete Sicherheitsfunktion impliziert und zu jeder Sicherheitsfunktion mindestens eine funktionale Sicherheitsanforderung existiert. Die Sicherheitsfunktionen sind eine Maßnahme, um die Risiken, die gegen einen EVG gerichtet sind und sich aus den Bedrohungen ergeben, zu minimieren. Sie werden in das Produkt integriert, um die zu schützenden Werte vor dem Verlust der Verfügbarkeit, der Vertraulichkeit und der Integrität zu sichern.

2.3.7 Zusammenfassung der Sicherheitszusammenhänge

Mit dem Hintergrund des erklärten Begriffes kann man daher verallgemeinern, dass der EVG den Sicherheitsbedarf, der sich aus Bedrohungen, organisatorischen Sicherheitspolitiken und Sicherheitsannahmen ergibt, mittels seiner Sicherheitsfunktionen erfüllt und die Sicherheitsziele dabei die Aufgabe haben, den Zusammenhang herzustellen. Die folgende Grafik verdeutlicht den Zusammenhang.

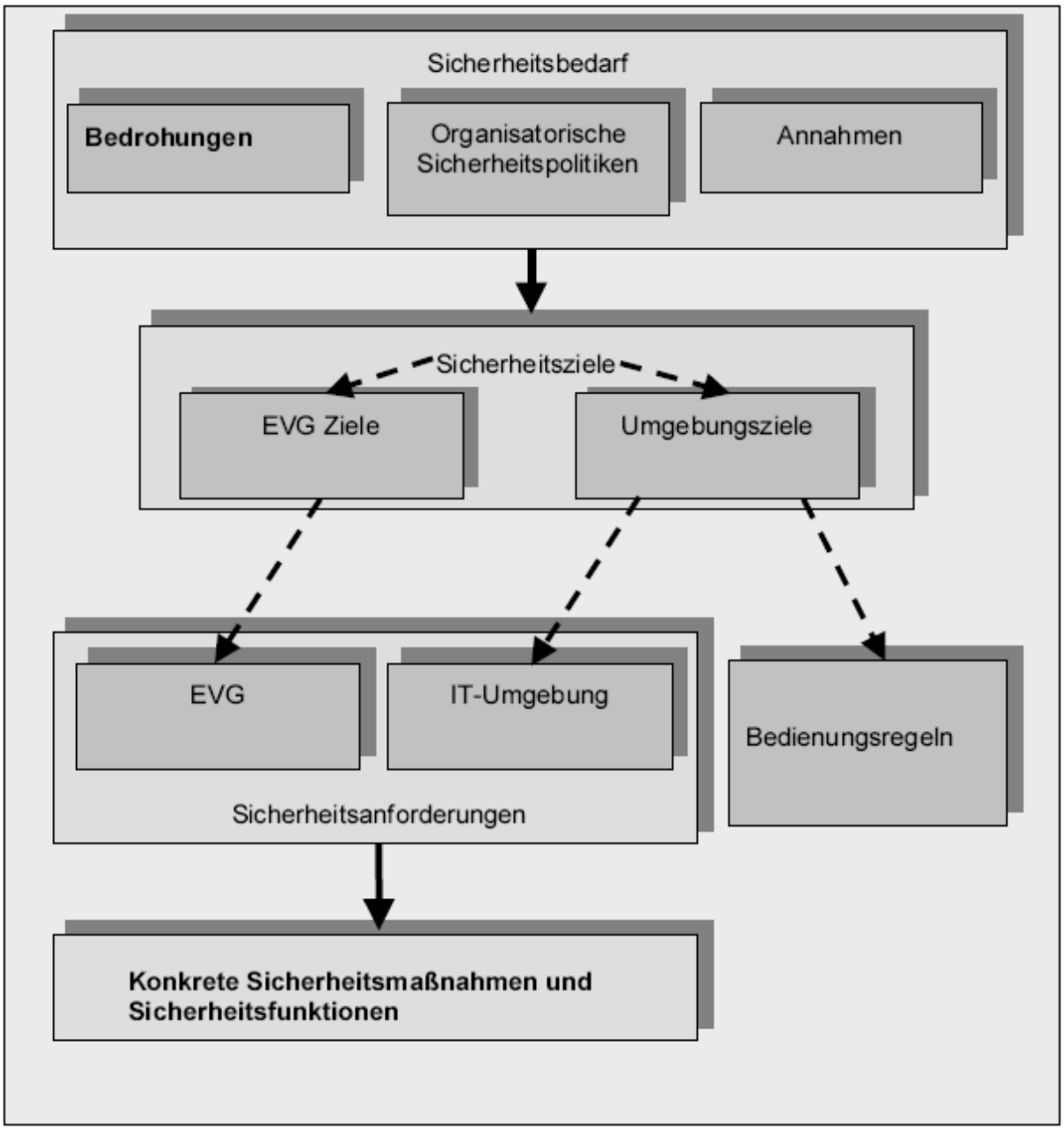

Sicherheitsbedarf
Bedrohungen
Organisatorische Sicherheitspolitiken
Annahmen
Sicherheitsziele
EVG Ziele
Umgebungsziele
EVG
IT-Umgebung
Bedienungsregeln
Sicherheitsanforderungen
Konkrete Sicherheitsmaßnahmen und Sicherheitsfunktionen

Abbildung 5

2.4 Die gesetzlichen Grundlagen

Die Umsetzung von konkreten Sicherheitsmaßnahmen und -funktionen, darf in Deutschland nicht gegen die folgenden gesetzlichen Regelungen verstoßen. Für IT-Produkte, die die Erstellung und Verwaltung von digitalen Schlüsseln beinhalten, gilt das Signaturgesetz. Das deutsche Signaturgesetz (SigG) oder auch Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste Gesetz - IuKDG) genannt, wurde am 13.06.1997 vom Bundestag beschlossen. Es legt fest, welche Rahmenbedingungen bei der Erstellung von Digitalen Signaturen als sicher gelten und bei welchen Rahmenbedingungen Fälschungen oder Verfälschung zuverlässig festgestellt werden können. Aufgrund des §16 des Signaturgesetzes wurde außerdem die Signaturverordnung (SigV) durch die Bundesregierung am 08.10.1997 erlassen, deren Begründung die Durchführungsbestimmungen und die Gewährleistung von sicheren digitalen Signaturen im Sinne des SigG regelt.

Darüber hinaus wurde von der Regulierungsbehörde für Telekommunikation und Post ein Maßnahmenkatalogentwurf herausgegeben, der die Umsetzung des Signaturgesetzes beschreibt. Dabei werden die Gestaltungsmöglichkeiten für die einzelnen technischen Komponenten und das organisatorische Umfeld erläutert, damit ein fälschungssicheres Gesamtsystem für digitale Signaturen geschaffen werden kann. Es werden explizit geeignete Kryptographiealgorithmen und Schnittstellenspezifikationen zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV dargestellt.

Natürlich müssen alle Produkte, die diesen gesetzlichen Grundlagen unterworfen sind, im Falle einer Evaluation den gesetzlichen Vorgaben bezüglich der Mindestanforderungen an die Vertrauenswürdigkeit und ihrer Sicherheitsfunktionen entsprechen. Die Sicherheitsfunktionen müssen aufgrund der verwendeten Zufallszahlen und Permutationsmechanismen die so genannte Stärke „hoch“ aufweisen.

3. Der Inhalt der Common Criteria

Die CC beinhalten Kriterien für die Prüfung und Bewertung von Sicherheitsanforderungen. Das Ziel der CC ist, eine Vergleichsmöglichkeit der Evaluationsergebnisse von Sicherheit in IT-Produkten zu schaffen. Um dies zu erreichen stellt CC eine gemeinsame Menge von Anforderungen an die Vertrauenswürdigkeit und Sicherheit zur Verfügung. Auf Basis dieser in Vertrauenswürdigkeitsklassen und Funktionalen Klassen eingeteilten Anforderungen kann das Evaluationsverfahren als Ergebnis eine Einordnung in das Maß für das Vertrauen – die EAL Stufe - erbringen.

„Die CC befassen sich mit dem Schutz von Informationen vor nicht-autorisierter Preisgabe, Modifizierung oder vor Zugangsverlust. Die diesen drei Bedrohungen zugewiesenen Schutzkategorien werden in der Regel mit Vertraulichkeit, Integrität und Verfügbarkeit bezeichnet. Die CC können auch auf Aspekte von IT-Sicherheit angewendet werden, die nicht in diese drei Kategorien fallen. Schwerpunkte der CC sind auf die Aktivitäten einer Person zurückzuführende Bedrohungen von Informationen, unabhängig davon, ob diese Aktivitäten böswillig sind oder nicht. Die CC gelten jedoch auch für einige nicht auf die Aktivitäten einer Person zurückzuführende Bedrohungen und sie können auch in anderen IT-Gebieten Anwendung finden, erheben aber außerhalb des eng umgrenzten Bereichs der IT-Sicherheit keinen Anspruch auf Kompetenz.“ [13)]

Aus obigem Auszug aus den Common Criteria lässt sich folgende Zuordnung treffen:

Bedrohung	Schutzkategorie
Nicht-Autorisierte Preisgabe	Vertraulichkeit
Modifizierung	Integrität
Zugangsverlust	Verfügbarkeit

Tabelle 2

Die CC sind in mehrere Teile gegliedert. Nach einer Einführung mit Definitionen und einer Übersicht, werden zuerst im Allgemeinen Modell Konzepte und deren Wechselwirkungen betrachtet. Es folgen eine Erläuterung der Anforderungen und Evaluationsergebnisse, sowie entsprechende Anhänge. Danach werden die einzelnen funktionalen Sicherheitskomponenten und die Anforderungen an die Vertrauenswürdigkeit mit ihren jeweiligen Klassen erklärt. Die Erklärungen der EAL und die jeweils dazugehörenden Anhänge schließen die CC ab.

Im Folgenden wird auf das Allgemeine Modell, Anforderungen, Ergebnisse und die Funktionalen und Vertrauenswürdigkeitsklassen näher eingegangen. Dabei wird zum größten Teil aus Primärliteratur zusammengefasst, um sich möglichst nah am Originaltext von CC zu orientieren. Dieses Kapitel soll eine verkürzte, aber prägnante Zusammenfassung der CC darstellen.

3.1 Das Allgemeine Modell

Das Allgemeine Modell veranschaulicht Konzepte der Sicherheit auf hoher Ebene und deren Wechselbeziehungen. Um den Sachverhalt vollständig zu verstehen, werden die Sicherheitszusammenhänge des zweiten Kapitels vorausgesetzt. Die folgende Grafik verdeutlicht in diesem Kontext noch einmal den Zusammenhang zwischen dem Interesse des Eigentümers, Bedrohungen und Risiken für das IT-Produkt zu reduzieren und dem Missbrauchsgedanken des Urhebers von Bedrohungen.

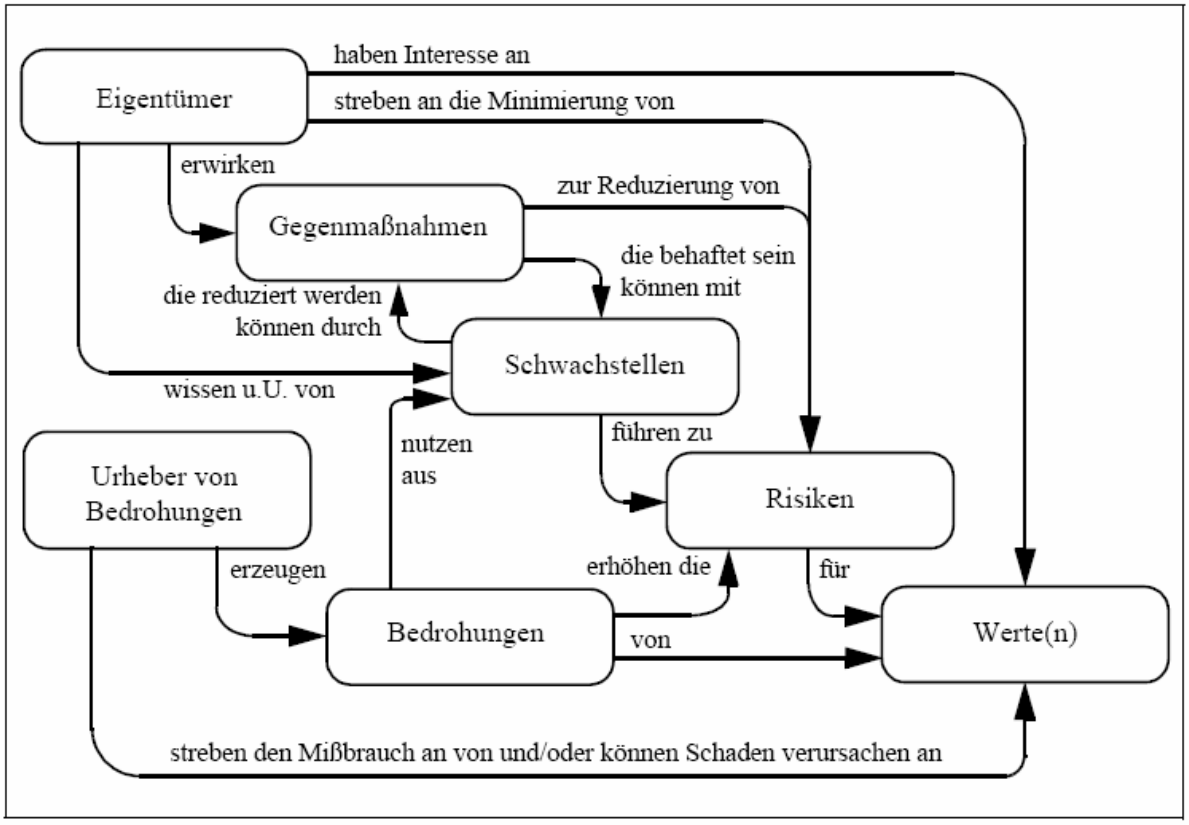


Abbildung 6

Die Grafik zeigt, dass der Eigentümer eines IT-Produkts dessen Werte schützen will. An diesen Werten sind aber auch eventuelle Urheber von Bedrohungen interessiert und sie trachten danach, die Werte zu manipulieren oder zu missbrauchen. Schäden, die durch diese Bedrohungen entstehen können sind die schon genannten Verluste der Vertraulichkeit, der Integrität und der Verfügbarkeit. Eine Analyse der Bedrohungen muss zeigen, welche dieser drei Verluste in der Umgebung des IT-Produkts möglich sind. Aus den Analyseergebnissen ergeben sich die möglichen Risiken für das Produkt und geeignete Gegenmaßnahmen, um die Schwachstellen zu reduzieren, damit die Sicherheitspolitiken der Eigentümer umgesetzt werden können. Natürlich kann ein minimales Restrisiko niemals ausgeschlossen werden. Daher kann das Ziel nur die Minimierung der Risiken sein.

Sind die Risiken minimiert, muss die Vertrauenswürdigkeit in den EVG geprüft und bewertet werden, damit der Eigentümer einen geeigneten Nachweis erhält. Es handelt sich dabei um das Vertrauen, dass die Gegenmaßnahmen das Risiko für eine Bedrohung der Werte eines Produktes minimieren. Der Eigentümer erhält durch die

Prüfung und Bewertung objektive und wiederholbare Ergebnisse, mit denen er das Vertrauen in sein Produkt belegen und rechtfertigen kann.

Anhand von Vertrauenswürdigkeitskriterien identifiziert CC Entwurfs-Abstraktionsebenen für die funktionale Spezifikation. Zuerst muss ein Entwurf auf hoher Ebene, dann ein Entwurf auf niedriger Ebene und letztendlich die Implementierung von Statten gehen. Je nach Vertrauenswürdigkeitsstufe müssen die Entwickler eventuell zeigen, wie die Entwicklungsmethodik die CC Anforderungen an die Vertrauenswürdigkeit erfüllt. Dabei schreibt CC übrigens keine konkrete Entwicklungsmethodologie und kein konkretes Lebenszyklusmodell vor.

Die folgende Grafik zeigt, dass zuerst Evaluationskriterien festgelegt werden müssen, aus denen dann Sicherheitsanforderungen für den EVG entstehen. Nach den genannten Entwurfsstufen folgt dann die Implementierung des EVG. Der EVG wird danach evaluiert, wobei eine bestimmte Evaluationsmethodologie wie das CEM und ein Evaluationsschema benötigt werden. Sind die Evaluationsergebnisse dann zufrieden stellend, kann der EVG in Betrieb genommen werden.

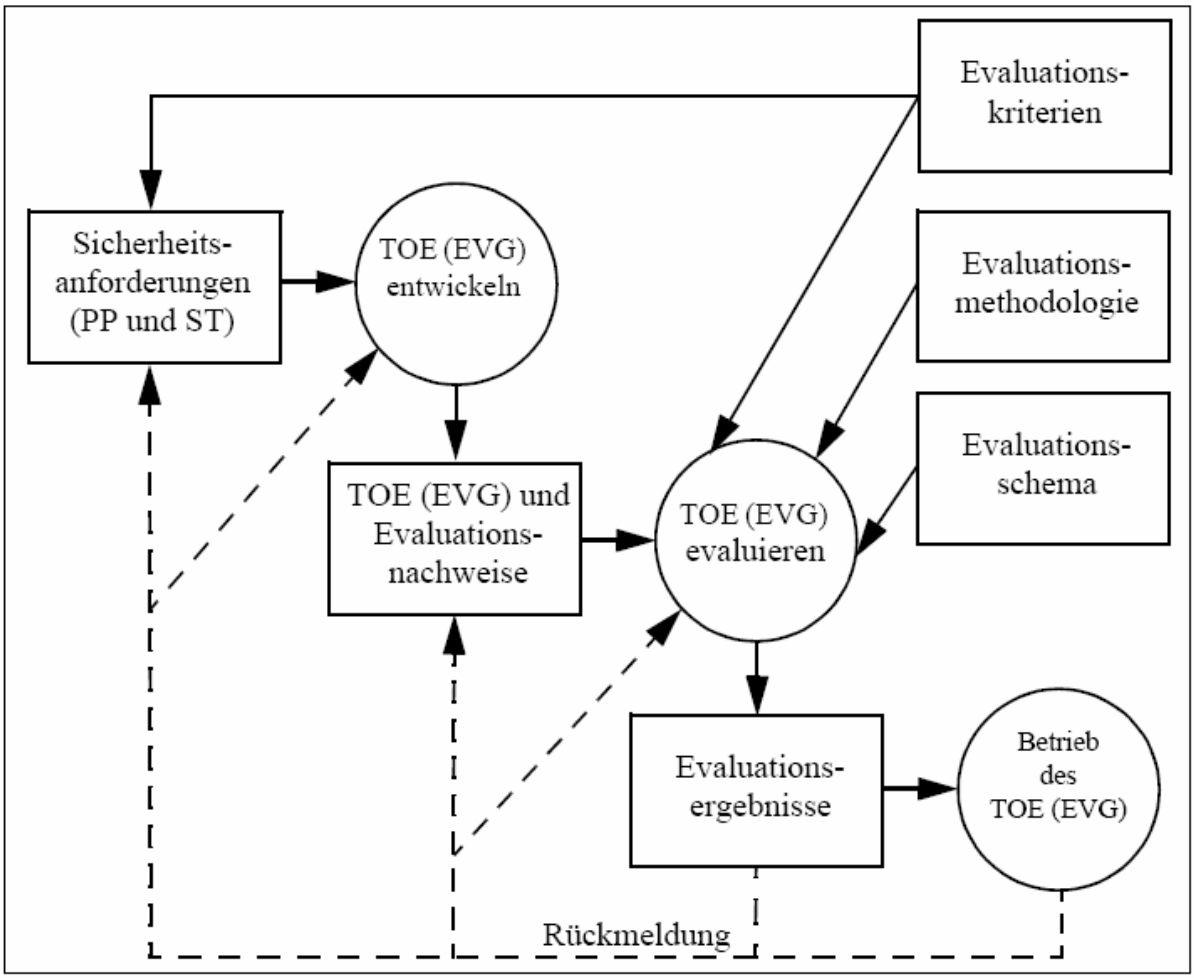


Abbildung 7

Die Festlegung der Sicherheitsanforderungen soll nach CC in verschiedenen Darstellungsebenen getroffen werden, um je nach dem Bedarf der Abstraktionsebene den EVG zu beschreiben. Eine Darstellungsebene soll eine durchdachte und überzeugende Darlegung enthalten, die zeigt, dass eine untere Ebene der höheren

entspricht. Außerdem muss die Darlegung vollständig, korrekt und in sich konsistent sein, um zusammen mit den höheren Ebenen die EVG-Korrektheit zu unterstützen. Für die Vertrauenswürdigkeit des EVG tragen Erklärungen bei, die die Übereinstimmung mit den Sicherheitszielen direkt nachweisen. Die unterschiedlichen Darstellungsebenen werden in der folgenden Grafik verdeutlicht:

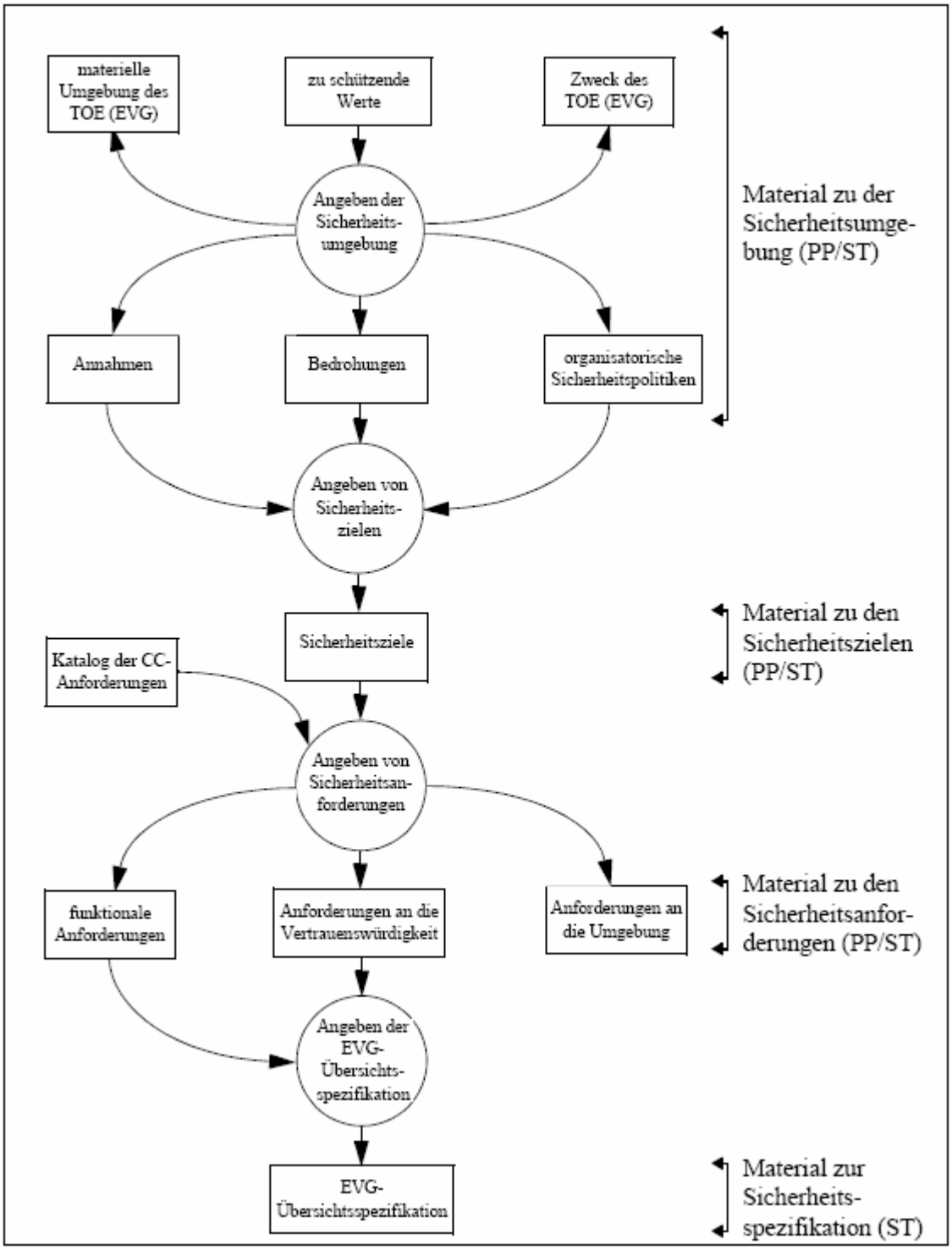


Abbildung 8

Das Bild veranschaulicht die Beziehungen einiger analytischer Ansätze zum Inhalt der Schutzprofile und Sicherheitsvorgaben und zeigt, wie die Sicherheitsanforderungen und

Spezifikationen bei der Entwicklung eines Schutzprofils oder einer Sicherheitsvorgabe abgeleitet werden können. Letztendlich entstehen alle Sicherheitsanforderungen aus Überlegungen, über den Zweck des EVG und die Umgebung, in der der EVG betrachtet wird.

Die CC enthalten eine hierarchische Einteilung der Sicherheitsanforderungen in Klassen, Familien und Komponenten.

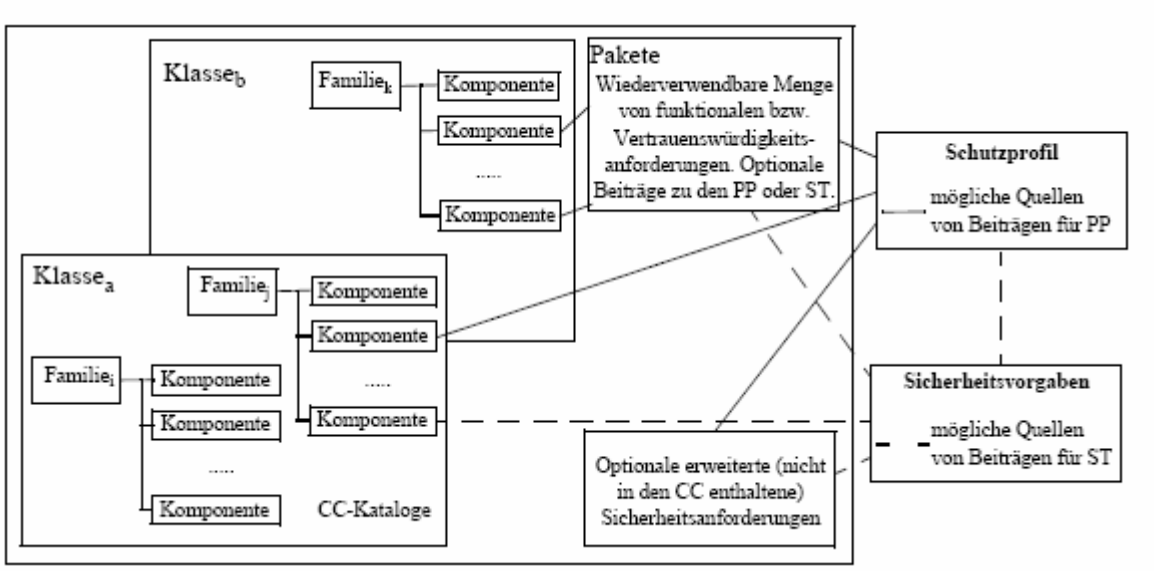


Abbildung 9

3.1.1 Klasse

Die allgemeinste Gruppe von Sicherheitsanforderungen wird als Klasse bezeichnet. Jedes Mitglied einer Klasse hat zwar dieselbe Zielrichtung, unterscheidet sich aber in der Abdeckung der Sicherheitsziele. Die Mitglieder einer Klasse nennt man Familie.

3.1.2 Familie

Eine Gruppe von Mengen an Sicherheitsanforderungen wird Familie genannt, wenn sie gemeinsame Sicherheitsziele haben. Die Mitglieder einer Familie nennt man Komponenten. Für die Mengen an funktionalen Sicherheitsanforderungen gilt, dass sie sich in der Betonung und Schärfe der Sicherheitsziele unterscheiden und aufeinander aufbauen können.

3.1.3 Komponente

„Eine Komponente beschreibt eine spezielle Menge von Sicherheitsanforderungen und ist die kleinste auswählbare Menge von Sicherheitsanforderungen, die in die in den CC definierte Struktur aufgenommen werden können. Die Komponenten in einer Familie können nach zunehmender Stärke bzw. Fähigkeit dem gleichen Zweck dienender Sicherheitsanforderungen geordnet sein. Die Menge kann jedoch auch aus verwandten

Komponenten bestehen, die in keiner hierarchischen Beziehung zueinander stehen. In manchen Fällen enthält die Familie nur eine Komponente, so daß sich eine Ordnung erübrigt. Die Komponenten sind aus einzelnen Elementen aufgebaut. Das Element ist die niedrigste Darstellungsebene von Sicherheitsanforderungen. Das Element ist eine unteilbare Sicherheitsanforderung, die mittels Prüfung und Bewertung verifiziert werden kann." [13)]

Es kann Abhängigkeiten zwischen Komponenten geben, die entstehen, wenn eine Komponente sich auf eine andere Komponente verlassen muss, weil sie alleine nicht ausreichend ist. Die Abhängigkeiten können innerhalb von Vertrauenswürdigkeitskomponenten oder funktionalen Komponenten und auch zwischen diesen beiden Komponentenarten bestehen. Die genaue Beschreibung der Abhängigkeiten zwischen den Komponenten ist Teil der CC-Komponentendefinitionen. Allerdings können diese Definitionen auch unter Anwendung von erlaubten Operationen angepasst werden, um eine bestimmte Sicherheitspolitik zu erfüllen oder einer bestimmten Bedrohung entgegenzuwirken. Die vier erlaubten Operationen sind die Iteration, die Zuweisung, die Auswahl und die Verfeinerung.

- Die **Iteration** erlaubt den mehrmaligen Gebrauch einer Komponente mit verschiedenen Operationen.

- Die **Zuweisung** erlaubt die Spezifikation eines Parameters, der bei Gebrauch der Komponente eingesetzt werden kann.

- Die **Auswahl** erlaubt die Spezifikation von Bestandteilen, die aus einer in der Komponente angegebenen Liste ausgewählt werden.

- Die **Verfeinerung** erlaubt das Hinzufügen von zusätzlichen Details beim Gebrauch der Komponente.

3.1.4 Paket

Das Paket ist eine als Zwischenstufe verwendete Zusammenstellung von einzelnen Komponenten, die die Darstellung einer Menge von funktionalen Anforderungen und Vertrauenswürdigkeitsanforderungen erlaubt. Die Anforderungen müssen eine identifizierbare Teilmenge von Sicherheitszielen erfüllen und diesen wirklich und wirksam genügen. Aus Paketen können größere Pakete, Schutzprofile und Sicherheitsvorgaben aufgebaut werden. Beispielsweise sind die EAL vordefinierte Vertrauenswürdigkeitspakete, die eine Grundmenge von Vertrauenswürdigkeitsanforderungen an die Prüfung und Bewertung eines EVG darstellen und jeweils eine konsistente Menge bilden.

3.1.5 Schutzprofil

Ein Schutzprofil / Protection Profile (PP) besteht aus einer Menge von Sicherheitsanforderungen für Standard-Sicherheitsprobleme einer Produktgruppe. Die PP fassen die Anforderungen an die Funktionalität und an die Vertrauenswürdigkeit zusammen und mittels eines ausführlichen Beschreibungsteils werden die Bedrohungen den Anforderungen gegenübergestellt. Der Beschreibungsteil stellt damit das Sicherheitskonzept dar. Für eine Menge von EVG erlaubt ein PP eine implementierungsunabhängige Darstellung von Sicherheitsanforderungen, die eine Menge von Sicherheitszielen vollständig abdecken. Ein PP kann aber durch die daraus ableitbaren Sicherheitsvorgaben auf einen konkreten EVG zugeschnitten werden. Das PP soll dadurch wieder verwendbar sein.

„Durch die Verwendung von Schutzprofilen wird daher der Aufwand bei der Erstellung von Sicherheitsvorgaben für konkrete IT-Produkte oder Systeme erheblich reduziert." [17)]

3.1.6 Sicherheitsvorgaben

Die Sicherheitsvorgaben / Security Targets (ST) enthalten eine Menge von Sicherheitsanforderungen, die durch Verweis auf ein PP erstellt, oder explizit dargelegt werden. Die Sicherheitsanforderungen können dabei auch direkt auf funktionale Komponenten oder Vertrauenswürdigkeitskomponenten verweisen. Mittels der ST können konkrete EVG-Sicherheitsanforderungen dargestellt werden, die für die Erfüllung der Sicherheitsziele wirksam sind. In einem ST befindet sich außerdem die EVG-Übersichtsspezifikation und die Sicherheitsanforderungen und –ziele, sowie deren Erklärungen. Die ST bilden die Grundlage dafür, dass alle an einer Evaluation beteiligten Seiten hinsichtlich der von einem EVG gebotenen Sicherheit übereinstimmen.

3.2 Evaluationsergebnisse und Anforderungen an die Evaluation

Aus der Evaluierung eines PP ergeben sich Evaluationsergebnisse, die in Katalogen festgehalten werden. Erst danach, wenn ein PP geprüft und bewertet wurde, kann ein ST evaluiert werden. Auch hier entstehen bei der Prüfung und Bewertung Zwischenergebnisse, die im Rahmen der EVG-Evaluation weiter genutzt werden.

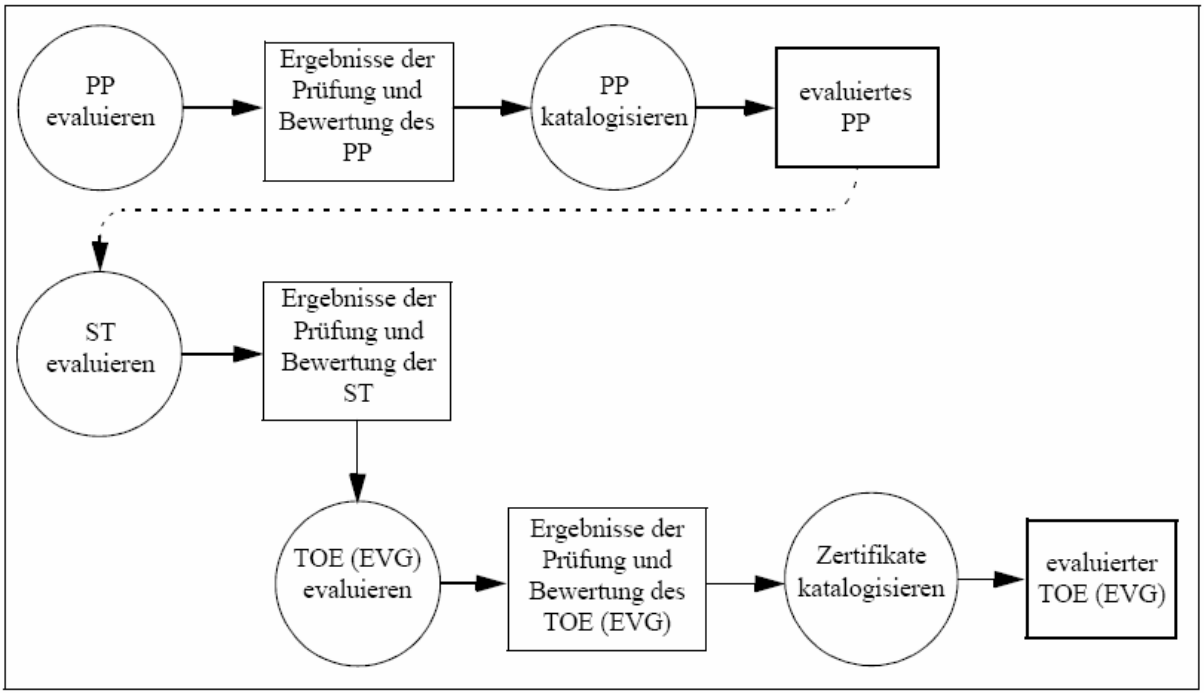


Abbildung 10

Wichtig ist, dass die Prüfung und Bewertung objektive und wiederholbare Ergebnisse liefert, damit eine sinnvolle Grundlage für die Anerkennung von Zertifikaten gegeben ist. Dies ist nur durch gemeinsame Evaluationskriterien lösbar, die den Sinn haben, dass ein möglichst objektiver Maßstab erreicht werden kann. Die CC enthalten die Evaluationskriterien, die es einem Evaluator erlauben auszusagen, ob ein PP vollständig, konsistent und technisch stimmig ist und sich daher zum Gebrauch als Darlegung der Anforderungen an einen EVG eignen. Eine Beurteilung auf Basis von CC ist das Ergebnis einer speziellen Art der Untersuchung der Sicherheitseigenschaften eines EVG.

Die folgenden Anforderungen müssen dabei für PP und ST eingehalten werden:

- Alle EVG-Anforderungen in PP und ST müssen nach dem Muster der Sicherheitskomponenten und Vertrauenswürdigkeitskomponenten dargestellt werden.

- Die Evaluation des PP muss zu der Aussage „akzeptiert“ oder „abgelehnt“ führen.

- Ein PP, welches als „akzeptiert“ gilt, kann in ein Register aufgenommen werden.

Außerdem ist der Evaluator durch Anwendung der CC bei der Prüfung und Bewertung des EVG in der Lage, Aussagen darüber zu machen, ob die funktionalen

Anforderungen und die Sicherheitsziele des EVG durch die spezifizierten Sicherheitsfunktionen erfüllt werden und ob die Implementierung der spezifizierten Sicherheitsfunktionen des EVG korrekt ist.

Als Ergebnis der Evaluation steht dann eine Aussage, die beschreibt bis zu welchem Grad man dem EVG vertrauen kann, die Anforderungen zu erfüllen. Wie mit dem Ergebnis der Evaluation weiter verfahren wird, ist unterschiedlich. Zum einen können Produkte auf stufenweise steigenden Komplettierungsebenen evaluiert und katalogisiert werden, bis betriebsbereite Systeme erreicht sind. Zum anderen können diese einer Prüfung und Bewertung in Verbindung mit einer Systemakkreditierung unterzogen werden.

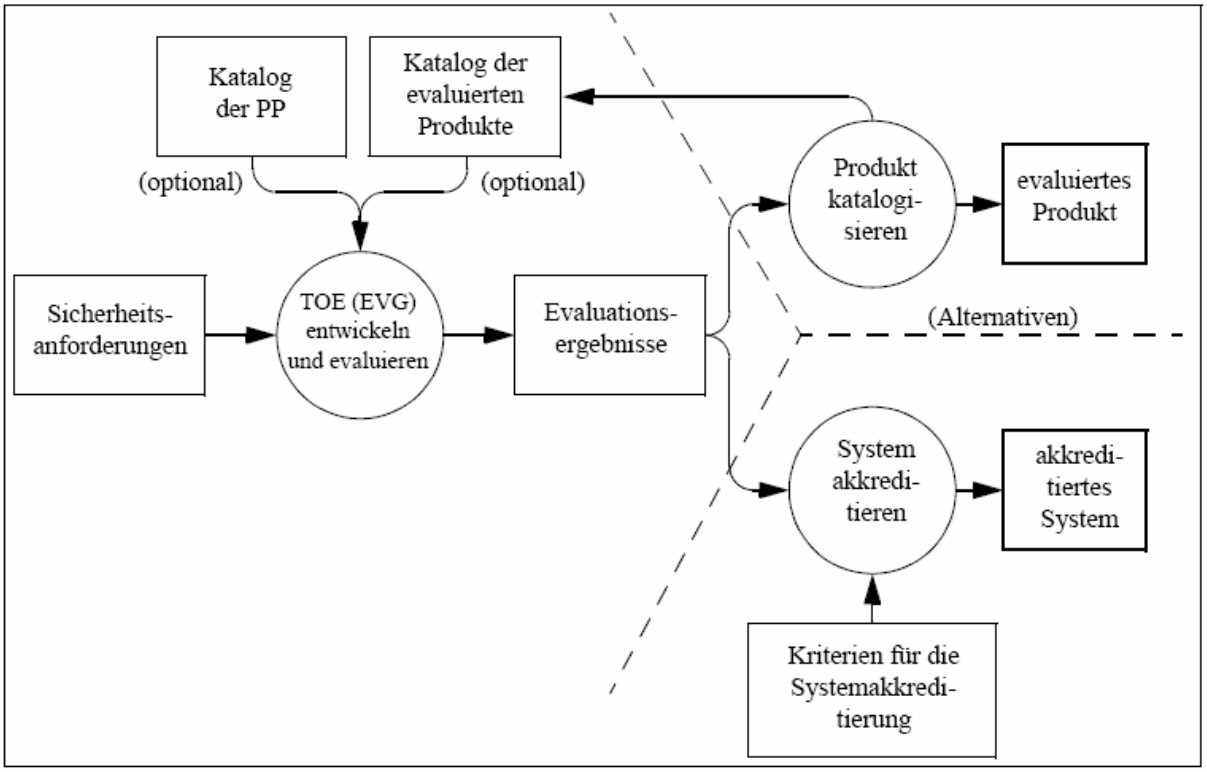


Abbildung 11

3.3 Die Funktionalen Klassen

Im Allgemeinen Modell der CC wurde schon erklärt, dass die CC eine hierarchische Einteilung der Sicherheitsanforderungen in Klassen, Familien und Komponenten enthalten. So verhält es sich auch bei den funktionalen Anforderungen, die in Klassen, Familien und Komponenten dargestellt sind. Dieses Kapitel soll zeigen, wie Inhalt und Form der funktionalen Anforderungen definiert sind. Das folgende Schema zeigt die Einteilung einer Funktionalen Klasse in Klassenname, Klasseneinführung und funktionale Familien.

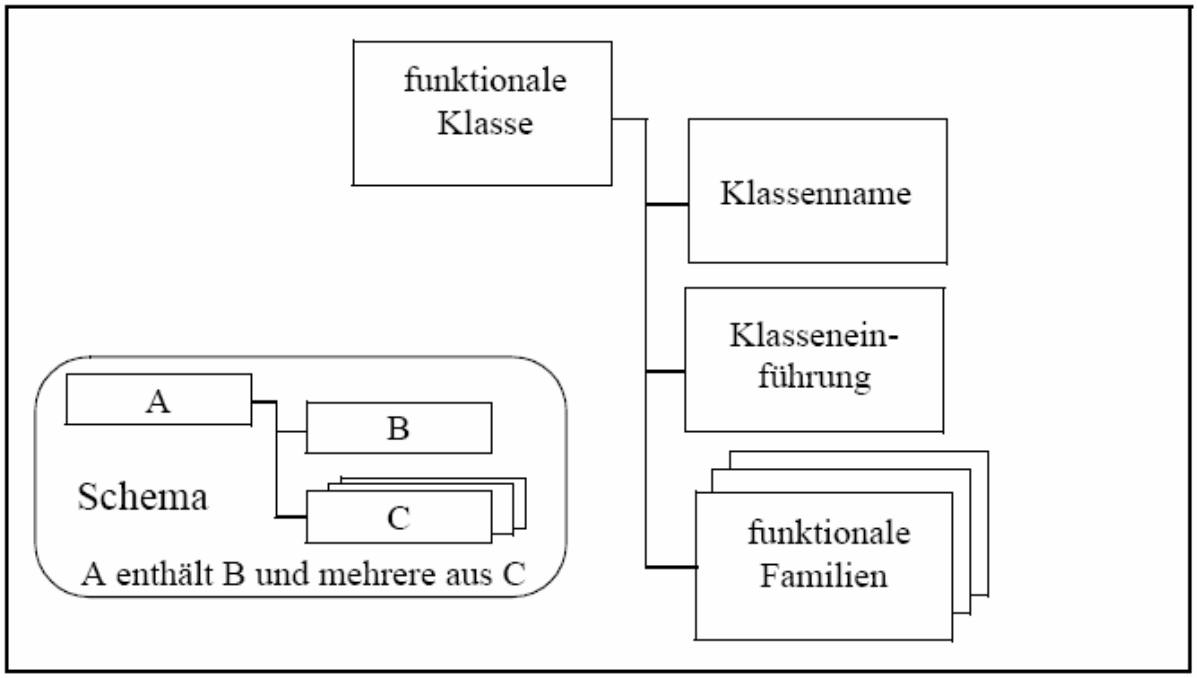


Abbildung 12

Klassenname: Durch einen eindeutigen Klassennamen wird die Klasse identifiziert und kategorisiert. Ein Kurzname aus drei Zeichen wird den Klassennamen im Folgenden abkürzen. Zum Beispiel wird die Klasse „Sicherheitsprotokollierung" mit dem Kürzel „FAU" gekennzeichnet. Alle Funktionalen Klassen beginnen mit einem „F" für „Functional".

Klasseneinführung: In ihr wird eine allgemeine Zielrichtung bzw. der Ansatz erläutert, mit dem die Familien die Sicherheitsziele erfüllen. Außerdem enthält sie ein Bild, das die Familien in dieser Klasse und die Hierarchie der Komponenten in jeder Familie beschreibt.

Funktionale Familie: Die Funktionale Familie beschreibt eine Menge von Sicherheitsanforderungen, durch einen Familiennamen, ein Familienverhalten, eine Komponentenabstufung, das Management, die Protokollierung und die Komponenten.

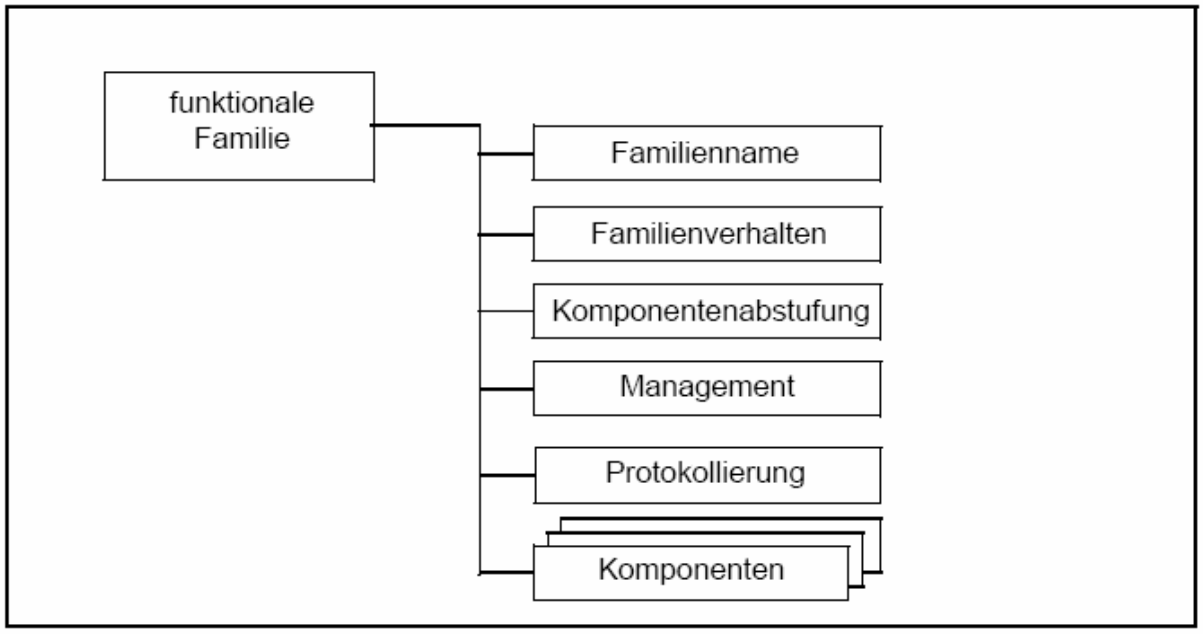


Abbildung 13

Familienname: Wie der Klassenname ist auch der Familienname eindeutig und identifizierend. Die Information zur Kategorie besteht aus einem sieben Zeichen langem Kürzel. Die ersten drei Zeichen entsprechen dem Klassennamen, dann folgt ein Unterstrich und zuletzt der Kurzname der Familie aus drei Zeichen. Beispielsweise wird die Familie „Analyse der Sicherheitsprotokollierung" mit dem Kürzel FAU_SAA bezeichnet.

Familienverhalten: Das Familienverhalten ist eine verbale Beschreibung der Sicherheitsziele einer funktionalen Familie und eine allgemeine Beschreibung der funktionalen Anforderungen.

Komponenten-abstufung: Da eine funktionale Familie eine oder mehrere Komponenten enthält, ist es nötig, die Beziehungen zwischen den Komponenten in der Komponentenabstufung zu erläutern. Normalerweise wird dies auch mittels einer grafischen Übersicht veranschaulicht.

Management: Die Managementanforderungen enthalten Informationen über Managementaktivitäten, die der Verfasser von PP/ST beachten sollte.

Protokollierung: Um die Protokollierung zu standardisieren, enthalten die Anforderungen an die Protokollierung protokollierbare sicherheitsrelevante Ereignisse. Ein Protokollierungshinweis könnte folgendermaßen aussehen:

„Minimal – erfolgreicher Gebrauch des Sicherheitsmechanismus;
Einfach – jeder Gebrauch des Sicherheitsmechanismus sowie die beteiligten Sicherheitsattribute betreffende Informationen;

Detailliert – jede Änderungen der Konfiguration des Mechanismus, einschließlich der Konfigurationswerte vor und nach der Änderung." [13)]

Komponenten: Eine Komponente beschreibt eine Menge von Sicherheitsanforderungen durch eine Komponenten-identifikation, ein oder mehrere funktionale Elemente und Abhängigkeiten.

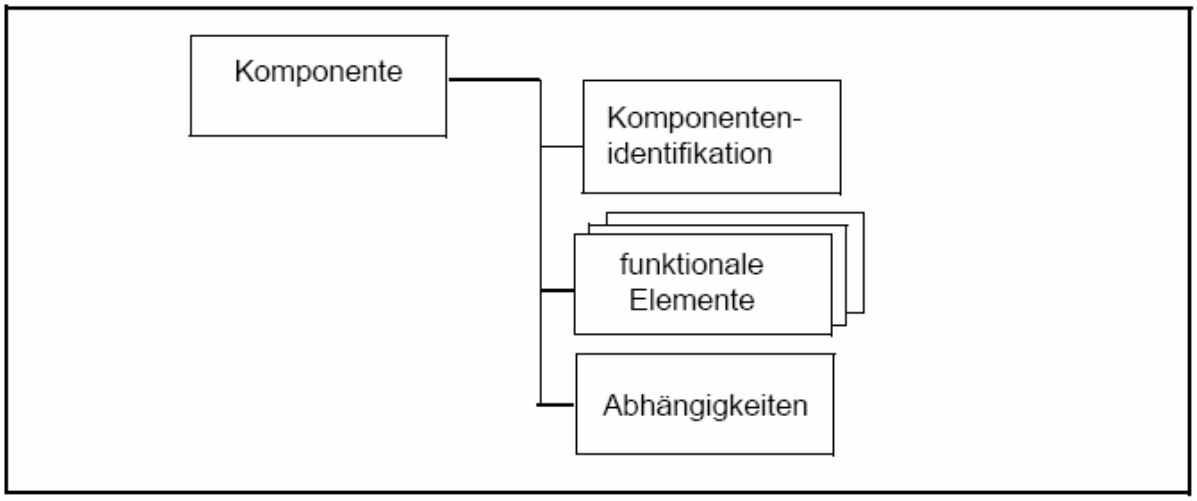


Abbildung 14

Komponenten-identifikation: Eine Komponentenidentifikation beinhaltet Informationen über Identifikation, Kategorisierung und Registrierung einer Komponente sowie eventuelle Querverweise. Dabei werden ein eindeutiger Name und eine Hierarchieliste aller Komponenten, zu denen die Komponente hierarchisch ist, angegeben.

Funktionale Elemente: Ein Funktionales Element ist eine funktionale Sicherheitsanforderung, die in sich abgeschlossen ist und daher nicht mehr weiter unterteilt werden kann.

Abhängigkeiten: Wenn eine funktionale Komponente allein nicht ausreichend ist und sich daher auf andere Komponenten verlassen muss, müssen diese Abhängigkeiten beschrieben werden. Es können auch Abhängigkeiten mit Vertrauenswürdigkeitsklassen bestehen.

Nachdem nun ein ausführlicher Überblick über die Bestandteile der Funktionalen Klassen gegeben wurde, wird im Folgenden auf die vordefinierten Klassen näher eingegangen.

3.3.1 Sicherheitsprotokollierung

Die Klasse Sicherheitsprotokollierung (Security Audit) wird mit dem Kürzel **FAU** bezeichnet. Sie besteht aus sechs Familien, die funktionale Sicherheitsanforderungen zur Erstellung, Speicherung, Schutz, Verarbeitung, Verwaltung und Auswertung des Protokolls, sowie Reaktion auf protokollierte Aktionen enthalten.

- Die **Automatische Reaktion der Sicherheitsprotokollierung (FAU_ARP)** legt die auszuführende Reaktion für den Fall fest, dass ein Ereignis entdeckt wird, dass auf eine potentielle Sicherheitsverletzung hindeutet.

- Die **Generierung der Sicherheitsprotokolldaten (FAU_GEN)** definiert Anforderungen an die Protokollierung des Auftretens sicherheitsrelevanter Ereignisse, die unter EVG-Sicherheitsfunktionskontrolle ausgeführt werden. Außerdem werden die Stufen der Protokollierung identifiziert und die Ereignisarten aufgezählt, die durch die EVG-Sicherheitsfunktionen protokollierbar sein müssen. Weiterhin wird die Mindestmenge der protokollbezogenen Informationen angegeben, die innerhalb der verschiedenen Arten von Protokollaufzeichnungen bereitgestellt werden müssen.

- Die **Analyse der Sicherheitsprotokollierung (FAU_SAA)** legt Anforderungen an automatische Mittel zur Analyse von Systemaktivitäten fest und überprüft Protokolldaten auf mögliche oder tatsächliche Sicherheitsverletzungen. Die Analyse kann bei der Angriffserkennung und der automatischen Reaktion auf drohende Sicherheitsverletzungen unterstützen.

- Die **Durchsicht der Sicherheitsprotokollierung (FAU_SAR)** identifiziert die Anforderungen an Protokollierungswerkzeuge, die den autorisierten Benutzern zur Durchsicht der Protokolldaten zur Verfügung stehen sollen.

- Die **Ereignisauswahl für die Sicherheitsprotokollierung (FAU_SEL)** definiert die zu protokollierenden Anforderungen zur Auswahl der Ereignisse während des EVG-Betriebs. Außerdem werden Anforderungen zum Aufnehmen oder Ausschließen von Ereignissen in die oder aus der Menge der protokollierbaren Ereignisse festgelegt.

- Die **Ereignisspeicherung der Sicherheitsprotokollierung (FAU_STG)** definiert die Anforderungen an die EVG-Sicherheitsfunktionen zur Erstellung und Erhaltung sicherer Protokolle.

3.3.2 Kommunikation

Die Klasse Kommunikation (Communication) wird mit dem Kürzel FCO bezeichnet. Sie besteht aus zwei Familien, die funktionale Sicherheitsanforderungen zur Identität der am Datenaustausch beteiligten Seiten und zum Sende- und Empfangsnachweis bereitstellen.

- Die Nichtabstreitbarkeit der Urheberschaft (FCO_NRO) stellt sicher, dass der Urheber einer Nachricht nicht erfolgreich bestreiten kann sie versendet zu haben. Dies erfordert allerdings, dass die EVG-Sicherheitsfunktionen eine Methode bereitstellen, die sicherstellt, dass einem Subjekt, das während eines Datenaustausches Informationen empfängt, der Urheberschaftsnachweis dieser Informationen zur Verfügung gestellt wird.

- Die Nichtabstreitbarkeit des Empfangs (FCO_NRR) stellt sicher, dass der Empfänger der Informationen nicht erfolgreich bestreiten kann sie erhalten zu haben. Auch dies erfordert, dass die EVG-Sicherheitsfunktionen eine Methode bereitstellen, die sicherstellt, dass einem Subjekt, das während eines Datenaustausches Informationen übermittelt, einen Empfangsnachweis der Informationen zur Verfügung steht.

Diese Klasse hat einen starken Bezug zur Kryptografie, da sie auf die Telekommunikation zugeschnitten ist.

3.3.3 Kryptografische Unterstützung

Die Klasse Kryptografische Unterstützung (Cryptographic Support) wird mit dem Kürzel FCS bezeichnet. Diese Klasse wird nur dann verwendet, wenn der EVG kryptographische Funktionen enthält, die als Hardware, Firmware und/oder Software implementiert sein können.

- Die Familie Kryptographisches Schlüsselmanagement (FCS_CKM) behandelt die Aspekte des Managements kryptographischer Schlüssel. Diese Familie ist zur Unterstützung des Lebenszyklus gedacht und definiert deshalb Anforderungen an die Generierung kryptographischer Schlüssel, Verteilung kryptographischer Schlüssel, Zugriff auf kryptographische Schlüssel und Zerstörung kryptographischer Schlüssel.

- Die Familie Kryptographischer Betrieb (FCS_COP) befasst sich mit der Anwendung des kryptographischen Schlüssels während des Betriebs. Einige typische kryptographische Operationen sind unter anderem Datenverschlüsselung und/oder -entschlüsselung, Generierung und/oder Verifizierung von digitalen Unterschriften, kryptographische Prüfsummengenerierung für die Integrität und/oder Prüfsummenverifizierung, sichere Hash-Funktionen, Verschlüsselung und/oder Entschlüsselung des kryptographischen Schlüssels und die Vereinbarung von kryptographischen Schlüsseln.

3.3.4 Schutz der Benutzerdaten

Die Klasse Schutz der Benutzerdaten (User Data Protection) wird mit dem Kürzel **FDP** bezeichnet. Sie besteht aus 13 Familien, die funktionale Sicherheitsanforderungen zur Zugriffskontrolle, Informationsflusskontrolle, Attributverwaltung, Schutz der gespeicherten Daten gegen unbefugte Wiederaufbereitung, Integritätsüberwachung von gespeicherten Daten, Rückgängigmachen von Aktionen und Datenübertragung bereitstellen.

Die Familien in dieser Klasse sind in vier Gruppen aufgeteilt:

a) Sicherheitsfunktionspolitiken zum Schutz der Benutzerdaten:

- Die **Zugriffskontrollpolitik (FDP_ACC)** legt funktionale Sicherheitspolitiken für die Zugriffskontrolle fest und definiert den Kontrollanwendungsbereich der Politiken, die den identifizierten Teil der Zugriffskontrolle der EVG bilden.

- Die **Politik der Informationsflußkontrolle (FDP_IFC)** identifiziert die funktionalen Sicherheitspolitiken für die Informationsflusskontrolle und legt den Anwendungsbereich der Kontrolle der Politiken fest, die den identifizierten Teil der TSP für Informationsflusskontrolle bilden.

b) Formen des Schutzes der Benutzerdaten:

- Die **Zugriffskontrollfunktionen (FDP_ACF)** beschreiben die Regeln für die besonderen Funktionen, die eine der Zugriffskontrollpolitiken implementieren können. FDP_ACC spezifiziert dabei den Anwendungsbereich der Kontrolle der Politik.

- Die **Funktionen der Informationsflußkontrolle (FDP_IFF)** beschreiben die Regeln der speziellen Funktionen, welche die in FDP_IFC genannten funktionalen Sicherheitspolitiken für die Informationsflusskontrolle implementieren.

- Die Familie **EVG-interner Transfer (FDP_ITT)** stellt Anforderungen bereit, die den Schutz von Benutzerdaten behandeln, wenn diese innerhalb eines EVG über einen internen Kanal übertragen werden.

- Der **Schutz bei erhalten gebliebenen Informationen (FDP_RIP)** stellt sicher, dass auf gelöschte Informationen nicht länger zugegriffen werden kann und dass neu erstellte Objekte keine Informationen enthalten, die nicht zugänglich sein sollten. Zu beachten ist, dass diese Familie den Schutz von Informationen erfordert, die logisch gelöscht oder freigegeben wurden, sich aber noch innerhalb des EVG befinden können.

- Die Operation **Rückgängig (FDP_ROL)** stellt die Fähigkeit bereit, die Auswirkungen einer Operation oder einer Reihe von Operationen rückgängig zu machen, um die Integrität der Benutzerdaten zu erhalten.

- Die **Integrität der gespeicherten Daten (FDP_SDI)** stellt die Anforderungen bereit, die den Schutz von Benutzerdaten betreffen, während diese innerhalb des Anwendungsbereichs der EVG-Sicherheitsfunktionskontrolle gespeichert sind.

c) Offline-Speicherung, Import und Export:

- Die **Datenauthentisierung (FDP_DAU)** stellt eine Methode bereit, welche die Gültigkeit einer speziellen Art von Daten garantiert. Darüber hinaus kann bei Weiterverwendung der Daten verifiziert werden, ob der Inhalt der Informationen gefälscht oder betrügerisch verändert wurde. Im Gegensatz zur Klasse FCO ist diese Familie zur Anwendung mit „statischen" Daten gedacht.

- Die Familie **Export nach außerhalb der TSF-Kontrolle (FDP_ETC)** definiert Funktionen zum Export von Benutzerdaten, so dass deren Sicherheitsattribute und Schutz entweder explizit erhalten oder ignoriert werden können, wenn diese einmal exportiert sind. Sie befasst sich außerdem mit Exportbegrenzungen und mit der Verknüpfung von Sicherheitsattributen mit den exportierten Benutzerdaten.

- Die Familie **Import von außerhalb der TSF-Kontrolle (FDP_ITC)** legt die Mechanismen zur Einführung der Benutzerdaten in den EVG fest, so dass diese über angemessene Sicherheitsattribute verfügen und angemessen geschützt sind. Sie befasst sich weiterhin mit Begrenzungen des Imports, der Festlegung gewünschter Sicherheitsattribute und der Interpretation von Sicherheitsattributen, die mit den Benutzerdaten verknüpft sind.

d) Inter-TSF-Kommunikation:

- Der **Schutz der Benutzerdatenvertraulichkeit bei Inter-TSF-Transfer (FDP_UCT)** legt die Anforderungen zur Sicherstellung der Vertraulichkeit von Benutzerdaten fest, wenn diese über einen externen Kanal zwischen unterschiedlichen EVG oder Benutzern in unterschiedlichen EVG übertragen werden.

- Der **Schutz der Benutzerdatenintegrität bei Inter-TSF-Transfer (FDP_UIT)** definiert die Anforderungen an die Integrität von Benutzerdaten während der Übertragung zwischen den EVG-Sicherheitsfunktionen und einem anderen vertrauenswürdigen IT-Produkt und an die Wiederherstellung nach erkennbaren Fehlern. Diese Familie überwacht zumindest die Integrität der Benutzerdaten auf Modifizierungen und unterstützt verschiedene Wege der Korrektur von festgestellten Integritätsfehlern.

Auch diese Klasse hat einen starken Bezug zur Kryptografie durch die genannten Themen. Der Schutz von Benutzerdaten wird vor allem durch die mit den Daten verbundenen Attribute vermittelt.

3.3.5 Identifikation und Authentifizierung

Die Klasse Identifikation und Authentifizierung (Identification and Authentication) wird mit dem Kürzel **FIA** bezeichnet. Sie besteht aus sechs Familien, die Attribute zur Identifizierung und Authentisierung, sowie Sicherheitsfunktionen zur Identifizierung und Authentisierung von Benutzern, Schutz der Authentisierungsdaten, Verhalten bei fehlgeschlagener Authentisierung und Qualität der Authentisierungsdaten bereitstellen.

- Die Familie **Authentisierungsfehler (FIA_AFL)** enthält Anforderungen zum Definieren von Werten für eine Anzahl von Authentisierungsversuchen und EVG-Sicherheitsfunktionsaktionen für den Fall, dass Authentisierungsversuche misslingen.

- Die **Definition der Benutzerattribute (FIA_ATD)** legt die Anforderungen an das Verknüpfen von Benutzersicherheitsattributen mit Benutzern entsprechend den Erfordernissen zur Unterstützung der EVG-Sicherheitspolitik fest.

- Die **Spezifikation der Geheimnisse (FIA_SOS)** definiert Anforderungen an Mechanismen, die festgelegte Qualitätsmetriken für gegebene Geheimnisse durchsetzen und Geheimnisse generieren, die die definierte Metrik erfüllen.

- Die **Benutzerauthentisierung (FIA_UAU)** Diese Familie legt die von den EVG-Sicherheitsfunktionen unterstützten Arten von Benutzerauthentisierungsmechanismen und die ebenfalls geforderten Attribute fest, auf denen die Benutzerauthentisierungsmechanismen basieren müssen.

- Die **Benutzeridentifikation (FIA_UID)** definiert die Bedingungen, unter denen von den Benutzern gefordert wird, sich vor Ausführung irgendwelcher anderer von den EVG-Sicherheitsfunktionen vermittelten Aktionen zu identifizieren.

- Die **Benutzer-Subjekt-Bindung (FIA_USB)** definiert Anforderungen zur Erzeugung und Erhaltung der Verknüpfung der Benutzersicherheitsattribute mit dem Subjekt, das für den Benutzer handelt.

3.3.6 Sicherheitsmanagement

Die Klasse Sicherheitsmanagement (Security Management) wird mit dem Kürzel **FMT** bezeichnet. Sie besteht aus sechs Familien und ist zur Spezifikation des Managements vielfältiger Aspekte der EVG-Sicherheitsfunktionen vorgesehen: Sicherheitsattribute, Sicherheitsfunktionsdaten und TSF-Funktionen.

- Das **Management der TSF-Funktionen (FMT_MOF)** erlaubt autorisierten Benutzern die Kontrolle über das Management von Funktionen in den EVG-Sicherheitsfunktionen.

- Das **Management der Sicherheitsattribute (FMT_MSA)** privilegiert autorisierte Benutzer, das Management der Sicherheitsattribute zu kontrollieren. Dieses Management kann auch Berechtigungen zur Ansicht und Modifizierung von Sicherheitsattributen einschließen.

- Das **Management der TSF-Daten (FMT_MTD)** erlaubt autorisierten Benutzern die Kontrolle über das Management der TSF-Daten wie Protokollinformationen, Uhr, Systemkonfiguration und andere Parameter der TSF-Konfiguration.

- Der **Widerruf (FMT_REV)** befasst sich mit dem Widerruf von Sicherheitsattributen verschiedener Einheiten innerhalb eines EVG.

- Der **Verfall der Sicherheitsattribute (FMT_SAE)** betrifft die Berechtigung, Zeitbegrenzungen für die Gültigkeit von Sicherheitsattributen zu vergeben.

- Die **Rollen im Sicherheitsmanagement (FMT_SMR)** dienen der Kontrolle der Zuweisung verschiedener Rollen an Benutzer.

3.3.7 Privatheit

Die Klasse Privatheit (Privacy) wird mit dem Kürzel **FPR** bezeichnet. Sie besteht aus vier Familien, die funktionale Sicherheitsanforderungen zur Unbeobachtbarkeit, Anonymität, Pseudonymität und Unverkettbarkeit bereitstellen.

- Die **Anonymität (FPR_ANO)** stellt den Schutz der Benutzeridentität sicher, so dass ein Benutzer ein Betriebsmittel oder einen Dienst ohne Preisgabe seiner Identität benutzen kann.

- Die **Pseudonymität (FPR_PSE)** garantiert, dass ein Benutzer ein Betriebsmittel oder einen Dienst zwar anonym benutzen kann, aber weiterhin noch für diesen Gebrauch verantwortlich gemacht werden kann.

- Die **Unverkettbarkeit (FPR_UNL)** stellt sicher, dass ein Benutzer die Betriebsmittel oder Dienste mehrfach benutzen kann, ohne dass andere in der Lage sind, diese Benutzungen miteinander zu verknüpfen und ihren Nutzen daraus zu ziehen.

- Die **Unbeobachtbarkeit (FPR_UNO)** garantiert, dass ein Benutzer ein Betriebsmittel oder einen Dienst benutzen kann, ohne dass andere beobachten können, dass dieses Betriebsmittel oder dieser Dienst benutzt wird.

„Diese funktionalen Sicherheitsanforderungen sind auf den Datenschutz ausgerichtet und wirken auf den ersten Blick ungewöhnlich oder gar paradox. Als Beispiel sei die Anonymität aufgeführt. Es entspricht der Erfahrung im Computerbereich, daß wenigstens der Administrator jede Aktivität von Benutzern überwachen kann (unabhängig davon, ob dies erlaubt ist oder nicht). Die Inanspruchnahme z.B. der Telefonseelsorge ist jedoch nur bei völliger Anonymität des Anrufenden sinnvoll. Daher dürfte der Vermittlungsrechner der Telefonseelsorge keine Möglichkeit bieten, die Telefonnummer des Anrufenden anzuzeigen, zu speichern oder in einer anderen Art und Weise bereitzustellen.“ [11)]

3.3.8 Schutz der EVG Sicherheitsfunktionen

Die Klasse Schutz der EVG Sicherheitsfunktionen (Protection of the Target of Evaluation Security Functions) wird mit dem Kürzel **FPT** bezeichnet. Sie besteht aus 16 Familien, die funktionale Sicherheitsanforderungen zum Test des Rechners, auf dem der EVG läuft, Selbsttest der Sicherheitsfunktionen, Administration der Sicherheitsfunktionen, Robustheit der Sicherheitsfunktionen, Vertraulichkeit, Integrität und Verfügbarkeit bei der Datenübertragung, Datenkonsistenz und zeitabhängige Attribute bereitstellen.

Diese Klasse unterscheidet drei signifikante TSF-Teile:

a) Die **abstrakte TSF-Maschine** ist eine virtuelle oder materielle Maschine, die zur Ausführung der konkreten zu evaluierenden TSF-Implementierung benutzt wird.

b) Die **TSF-Implementierung**, die die abstrakte Maschine zur Ausführung benutzt und die Mechanismen zur Durchsetzung der TSP implementiert.

c) Die **TSF-Daten**, welche die Systemverwaltungs-Datenbanken sind, die die Durchsetzung der TSP bestimmen.

- Der **Test der zugrunde liegenden abstrakten Maschine (FPT_AMT)** definiert Anforderungen, die die EVG-Sicherheitsfunktionstests zum Nachweis der Sicherheitsannahmen über die zugrunde liegende abstrakte Maschine, auf die sich die TSF verlassen, durchführen.

- Die Familie **Sicherer Fehlerzustand (FPT_FLS)** stellt sicher, dass der EVG seine Sicherheitspolitik im Fall von TSF-Fehlern aus identifizierten Kategorien nicht verletzen wird.

- Die **Verfügbarkeit von exportierten TSF-Daten (FPT_ITA)** beschreibt die Schutzregelungen gegen Verlust der Verfügbarkeit von TSF-Daten, die zwischen den TSF und einem entfernten, aber vertrauenswürdigen IT-Produkt bewegt werden.

- Die **Vertraulichkeit von exportierten TSF-Daten (FPT_ITC)** legt die Schutzregeln gegen die nichtautorisierte Preisgabe von TSF-Daten während der Übertragung zwischen den TSF und einem entfernten, aber vertrauenswürdigen IT-Produkt fest.

- Die **Integrität von exportierten TSF-Daten (FPT_ITI)** definiert die Schutzregeln gegen die nichtautorisierte Modifizierung von TSF-Daten während der Übertragung zwischen den TSF und einem entfernten vertrauenswürdigen IT-Produkt.

- Die Familie **EVG-interner TSF-Datentransfer (FPT_ITT)** stellt Anforderungen an den Schutz der TSF-Daten bereit, wenn diese über einen internen Kanal zwischen getrennten Teilen des EVG übertragen werden.

- Die Familie **Materieller TSF-Schutz (FPT_PHP)** stellt Anforderungen zur Verfügung, die garantieren, dass die TSF gegen materielle Manipulationen und Eingriffe geschützt sind und jegliche Versuche dieser Art sichtbar macht.

- Die **Vertrauenswürdige Wiederherstellung (FPT_RCV)** garantiert, dass die TSF feststellen können, dass der EVG ohne Schutzbloßstellung gestartet wurde und die Wiederherstellung nach Betriebsunterbrechungen ohne Schutzbloßstellung durchführen kann.

- Das **Erkennen von Wiedereinspielung (FPT_RPL)** betrifft das Erkennen der Wiedereinspielung verschiedener Arten von Einheiten und anschließenden Aktionen zur Korrektur. Im Falle einer Wiedereinspielung, wird diese hierdurch wirksam verhindert.

- Die **Referenzverbindung (FPT_RVM)** betrifft die Tatsache, dass ein herkömmlicher Referenzmonitor immer aktiv ist. Daher ist das Ziel für eine bestimmte funktionale Sicherheitspolitik sicherzustellen, dass alle Aktionen, die ein Durchsetzen der Politik erfordern, von den EVG-Sicherheitsfunktionen anhand der funktionalen Sicherheitspolitik validiert werden.

- Die **Bereichsseparierung (FPT_SEP)** stellt sicher, dass mindestens ein Sicherheitsbereich für die eigene Ausführung der TSF verfügbar ist und dass die TSF gegen externe Eingriffe und Manipulationen durch nichtvertrauenswürdige Subjekte geschützt sind. Das Einhalten der Anforderungen dieser Familie macht die TSF selbstschützend.

- Das **Protokoll zur Zustandssynchronisierung (FPT_SSP)** stellt Anforderungen, dass bestimmte kritische Sicherheitsfunktionen der TSF ein vertrauenswürdiges Protokoll benutzen und dass zwei verteilte EVG-Teile ihre Zustände nach einer sicherheitsrelevanten Aktion synchronisieren.

- Der **Zeitstempel (FPT_STM)** befasst sich mit den Anforderungen an eine Funktion für einen verlässlichen Zeitstempel innerhalb eines EVG.

- Die **Inter-TSF TSF-Datenkonsistenz (FPT_TDC)** definiert die Anforderungen an den gemeinsamen Gebrauch und die konsistente Interpretation der Attribute zwischen den TSF des EVG und einem anderen vertrauenswürdigen IT-Produkt.

- Die **Datenkonsistenz bei EVG-interner Datenreproduktion (FPT_TRC)** wird benötigt um sicherzustellen, dass die Konsistenz der TSF-Daten gegeben ist, wenn diese intern im EVG reproduziert werden.

- Der **TSF-Selbsttest (FPT_TST)** definiert die Anforderungen an den Selbsttest der TSF in Bezug auf den erwarteten korrekten Betrieb.

Diese Klasse hat ebenfalls einen starken Bezug zur Kryptografie.

3.3.9 Betriebsmittelnutzung

Die Klasse Betriebsmittelnutzung (Resource Utilization) wird mit dem Kürzel **FRU** bezeichnet. Sie besteht aus drei Familien, die funktionale Sicherheitsanforderungen zur Fehlertoleranz, Vorrang für bestimmte Dienstleistungen und Zuteilung von Ressourcen bereitstellen.

- Die **Fehlertoleranz (FRU_FLT)** garantiert, dass der EVG auch bei Auftreten von Fehlern weiter korrekt arbeitet.

- Die Familie **Priorität der Dienste (FRU_PRS)** stellt sicher, dass die Betriebsmittel den wichtigeren oder zeitkritischeren Aufgaben zugeteilt werden und nicht durch Aufgaben niedriger Priorität vereinnahmt werden können.

- Die **Betriebsmittelzuteilung (FRU_RSA)** stellt Begrenzungen für den Gebrauch der verfügbaren Betriebsmittel bereit und schützt deshalb den Benutzer vor einer Vereinnahmung der Betriebsmittel und vor einer Verweigerung von Diensten wegen nicht autorisierter Vereinnahmung von Betriebsmitteln.

3.3.10 EVG Zugriff

Die Klasse EVG Zugriff (Target of Evaluation Access) wird mit dem Kürzel **FTA** bezeichnet. Sie besteht aus sechs Familien, die funktionale Sicherheitsanforderungen zum Aufbau eines Login-Vorgangs, Mitteilung beim Login-Vorgang, Verwaltung und Sperrung des EVG bereitstellen.

- Die **Begrenzung des Anwendungsbereiches der auswählbaren Attribute (FTA_LSA)** definiert die Anforderungen zur Begrenzung des Anwendungsbereichs von Sicherheitsattributen einer Sitzung, die ein Benutzer auswählen kann.

- Die **Begrenzung bei mehreren gleichzeitigen Sitzungen (FTA_MCS)** legt Anforderungen zur Begrenzung der Anzahl gleichzeitiger, zum selben Benutzer gehörender Sitzungen fest.

- Das **Sperren der Sitzung (FTA_SSL)** definiert Anforderungen an die EVG-Sicherheitsfunktionen, die Fähigkeit des durch Sicherheitsfunktionen und Benutzer eingeleiteten Sperrens und wieder Entsperrens von interaktiven Sitzungen bereitzustellen.

- Die **EVG-Zugriffswarnmeldung (FTA_TAB)** legt Anforderungen zur Anzeige eines einstellbaren beratenden Warnhinweises für Benutzer für den angemessenen Gebrauch des EVG fest.

- Die **EVG-Zugriffshistorie (FTA_TAH)** definiert Anforderungen, damit die EVG-Sicherheitsfunktionen einem Benutzer nach erfolgreicher Sitzungseinrichtung eine Historie der erfolgreichen und fehlgeschlagenen Zugriffsversuche auf den Benutzeraccount anzeigen.

- Die **EVG-Sitzungseinrichtung (FTA_TSE)** stellt Anforderungen zur Verfügung, die für das Verweigern der Erlaubnis eines Benutzers, eine Sitzung mit dem EVG einzurichten zuständig sind.

3.3.11 Vertrauenswürdiger Pfad/Kanal

Die Klasse Vertrauenswürdiger Pfad/Kanal (Trusted Path/Channels) wird mit dem Kürzel **FTP** bezeichnet. Sie besteht aus zwei Familien, die funktionale Sicherheitsanforderungen für den Vertrauenswürdigen Pfad zwischen EVG und Benutzer und dem Vertrauenswürdigen Kanal zwischen entfernten Teilen eines EVG bereitstellen. Ein Vertrauenswürdiger Pfad oder Kanal sichert die Identifizierung und Authentisierung ab.

- Die Familie **Inter-TSF Vertrauenswürdiger Kanal (FTP_ITC)** legt Anforderungen zur Einrichtung eines vertrauenswürdigen Kanals zwischen den EVG-Sicherheitsfunktionen und anderen vertrauenswürdigen IT-Produkten für die Ausführung von sicherheitskritischen Operationen fest.

- Die Familie **Vertrauenswürdiger Pfad (FTP_TRP)** definiert die Anforderungen zum Einrichten und Aufrechterhalten einer vertrauenswürdigen Kommunikation zwischen den EVG-Benutzern und den EVG-Sicherheitsfunktionen.

3.4 Die Vertrauenswürdigkeitsklassen

Analog zu den Funktionalen Klassen erfolgt die Unterteilung der Vertrauenswürdigkeitsklassen (Assurance Classes) in Klassenname, Klasseneinführung und Vertrauenswürdigkeitsfamilien.

Klassenname: Ein eindeutiger Klassenname zeigt die von dieser Vertrauenswürdigkeitsklasse abgedeckten Aspekte an. Auch hier gilt, dass die Klasse durch einen Kurznamen aus drei Zeichen abgekürzt wird. Alle Vertrauenswürdigkeitsklassen beginnen mit einem „A" für „Assurance".

Klasseneinführung: In der Klasseneinführung wird die allgemeine Zielsetzung und die Zusammensetzung der Klasse beschrieben.

Vertrauenswürdigkeits-familien: Jede Vertrauenswürdigkeitsklasse enthält mindestens eine Vertrauenswürdigkeitsfamilie.

Analog zu den Funktionalen Klassen wird eine Vertrauenswürdigkeitsfamilie durch einen Familiennamen und eine Komponentenabstufung beschrieben. Darüber hinaus werden Ziele, Anwendungsbemerkungen und die dazugehörigen Vertrauenswürdigkeitskomponenten festgelegt.

Ziele: Die Zielsetzung der Vertrauenswürdigkeitsfamilie wird dargestellt. Die Beschreibung der Vertrauenswürdigkeitsfamilie ist dabei allgemein gehalten. Alle Details finden sich in der entsprechenden Vertrauenswürdigkeitskomponente.

Anwendungs-bemerkungen: Wenn Zusatzbemerkungen zur Vertrauenswürdigkeit nötig sind, werden sie in den Anwendungsbemerkungen informell festgehalten.

Vertrauenswürdigkeits-komponenten: Jede Vertrauenswürdigkeitsfamilie enthält mindestens eine Vertrauenswürdigkeitskomponente, die durch eine Komponentenidentifikation, Ziele, Anwendungsbemerkungen, Abhängigkeiten und Vertrauenswürdigkeitselemente definiert wird.

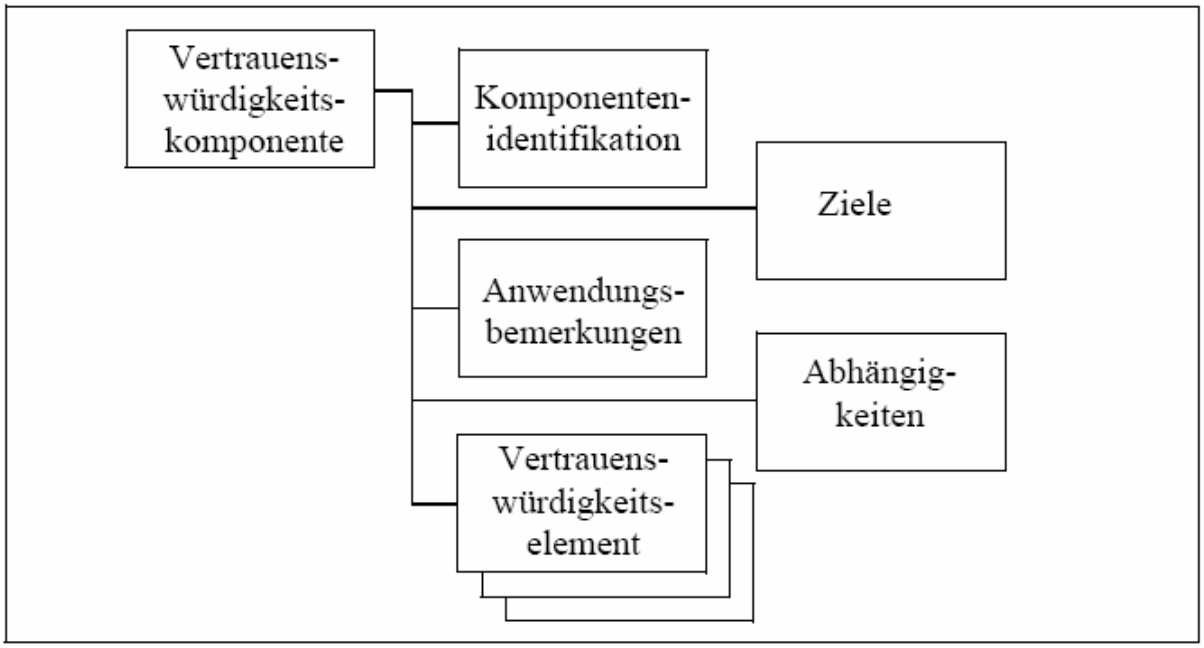


Abbildung 15

Komponenten-identifikation: Eine Komponentenidentifikation beinhaltet Informationen über Identifikation, Kategorisierung und Registrierung einer Komponente sowie eventuelle Querverweise. Dabei wird ein eindeutiger Name angegeben. Außerdem ist jede Vertrauenswürdigkeitskomponente einer Vertrauenswürdigkeitsfamilie zugeordnet, die das gleiche Sicherheitsziel aufweist wie die Komponente.

Ziele: Die Ziele der Vertrauenswürdigkeitskomponente beschreiben die besondere Zielsetzung der Komponente und geben eine detaillierte Erklärung der Ziele.

Anwendungs-bemerkungen: Falls vorhanden, werden Zusatzinformationen zur Erleichterung des Gebrauchs der Komponente in den Anwendungsbemerkungen beschrieben.

Abhängigkeiten: Wenn eine Vertrauenswürdigkeitskomponente allein nicht ausreichend ist und sich daher auf andere Komponenten verlassen muss, müssen diese Abhängigkeiten beschrieben werden. Jede Vertrauenswürdigkeitskomponente enthält ein vollständiges Verzeichnis ihrer Abhängigkeiten von anderen Vertrauenswürdigkeitskomponenten.

Vertrauenswürdigkeits-Elemente: Jede Vertrauenswürdigkeitskomponente verfügt über eine Menge von nicht mehr weiter zerlegbaren Elementen zur Vertrauenswürdigkeit.

Es gibt drei Mengen von Vertrauenswürdigkeitselementen. Zu einer von diesen Mengen muss ein Vertrauenswürdigkeitselement gehören:

- Elemente zu Entwickleraufgaben: Durch ein an die Elementnummer angehängtes „D" gekennzeichnet.

- Elemente zu Inhalt und Form des Nachweises: Durch ein an die Elementnummer angehängtes „C" gekennzeichnet.

- Elemente zu Evaluatoraufgaben: Durch ein an die Elementnummer angehängtes „E" gekennzeichnet.

Die ersten zwei Mengen definieren die Vertrauenswürdigkeitsanforderungen, die zur Darstellung der Verantwortlichkeiten des Entwicklers beim Vertrauenswürdigkeitsnachweis der Sicherheitsfunktionen angewendet werden. Sind die Anforderungen umgesetzt und erfüllt, stärkt der Entwickler das Vertrauen in das Produkt. Die Elemente des Evaluator legen seine Verantwortlichkeiten hinsichtlich der Prüfung und Bewertung fest. Dabei muss er zuerst die PP und ST validieren und dann den EVG hinsichtlich seiner funktionalen Anforderungen verifizieren.

Die dafür definierten Vertrauenswürdigkeitsklassen und die Ziele der Familien werden im Folgenden vorgestellt, wobei auf eine Ausführung über gegenseitige Abhängigkeiten weitgehend verzichtet wurde, um die Verständlichkeit zu erhöhen.

3.4.1 Prüfung und Bewertung des Schutzprofils

Die Klasse Prüfung und Bewertung des Schutzprofils (Protection Profile Evaluation) wird mit dem Kürzel APE bezeichnet. Das Ziel dieser Klasse ist die Prüfung und Bewertung, ob alle Aspekte des Schutzprofils in sich und untereinander sinnvoll und widerspruchsfrei sind.

- Die EVG-Beschreibung (APE_DES) soll dem Verständnis der EVG-Sicherheitsanforderungen dienen. Die Evaluation der EVG-Beschreibung muss zeigen, dass sie verständlich, in sich konsistent und konsistent mit allen anderen Teilen des PP ist.

- Die Sicherheitsumgebung (APE_ENV) legt fest, ob die in den PP enthaltenen IT-Sicherheitsanforderungen ausreichend sind und ob das zu lösende Sicherheitsproblem von allen an der Evaluation Beteiligten klar verstanden wird.

- Die PP-Einführung (APE_INT) enthält allgemeine Informationen, die zum Führen eines PP-Registers benötigt sind und Informationen zur Dokumentenverwaltung. Die

Evaluierung der PP-Einführung muss nachweisen, dass das PP korrekt identifiziert ist, und dass es konsistent mit allen anderen Teilen des PP ist.

- Die **Sicherheitsziele (APE_OBJ)** legen die beabsichtigte Reaktion auf das Sicherheitsproblem dar. Die Sicherheitsziele sind unterteilt in Sicherheitsziele für den EVG und in Sicherheitsziele für die Umgebung. Es muss für beide gezeigt werden, dass sie auf die identifizierten Bedrohungen, denen entgegengewirkt werden soll, und/oder die Politiken und Annahmen, die von ihnen erfüllt werden sollen, zurückverfolgbar sind.

- Die **EVG-Sicherheitsanforderungen (APE_REQ)** müssen nach der Evaluation bestätigen, dass sie in sich konsistent sind und zur Entwicklung eines EVG führen, der seine Sicherheitsziele erreicht. Diejenigen Sicherheitsziele, die an die Umgebung gerichtet sind, können dabei nicht erreicht werden und müssen deshalb explizit dargelegt werden und im Zusammenhang mit den EVG-Anforderungen evaluiert werden. Diese explizit dargelegten Anforderungen sind in der Familie APE_SRE enthalten.

- Die Familie **explizit dargelegte IT-Sicherheitsanforderungen (APE_SRE)** umfasst Anforderungen an die Evaluation, die erlauben festzustellen, dass die explizit dargelegten Anforderungen klar und eindeutig ausgedrückt sind.

3.4.2 Prüfung und Bewertung der Sicherheitsvorgaben

Die Klasse Prüfung und Bewertung der Sicherheitsvorgaben (Security Target Evaluation) wird mit dem Kürzel **ASE** bezeichnet. In dieser Klasse wird überprüft, ob die ST vollständig, konsistent und technisch stimmig sind und sich somit zum Gebrauch als Grundlage der entsprechenden EVG-Evaluation eignen. Einige Familienbeschreibungen ähneln hierbei den obigen Beschreibungen der Klasse APE.

- Die **EVG-Beschreibung (ASE_DES)** soll dem Verständnis der EVG-Sicherheitsanforderungen dienen. Die Evaluation der EVG-Beschreibung muss zeigen, dass sie verständlich, in sich konsistent und konsistent mit allen anderen Teilen des ST ist.

- Die **Sicherheitsumgebung (ASE_ENV)** legt fest, ob die in den ST enthaltenen IT-Sicherheitsanforderungen ausreichend sind und ob das zu lösende Sicherheitsproblem von allen an der Evaluation Beteiligten klar verstanden wird.

- Die **ST-Einführung (ASE_INT)** enthält Identifikations- und Hinweismaterial. Die Evaluierung der PP-Einführung muss nachweisen, dass das PP korrekt identifiziert ist, und dass es konsistent mit allen anderen Teilen des PP ist.

- Die **Sicherheitsziele (ASE_OBJ)** legen die beabsichtigte Reaktion auf das Sicherheitsproblem dar. Die Sicherheitsziele sind unterteilt in Sicherheitsziele für den EVG und in Sicherheitsziele für die Umgebung. Es muss für beide gezeigt werden, dass sie auf die identifizierten Bedrohungen, denen entgegengewirkt werden soll,

und/oder die Politiken und Annahmen, die von ihnen erfüllt werden sollen, zurückverfolgbar sind.

- Die **PP-Postulate (ASE_PPC)** müssen bei ihrer Prüfung und Bewertung feststellen, ob die ST eine korrekte Umsetzung des PP sind.

- Die **IT-Sicherheitsanforderungen (ASE_REQ)** müssen nach der Evaluation bestätigen, dass sie in sich konsistent sind und zur Entwicklung eines EVG führen, der seine Sicherheitsziele erreicht. Sie enthalten Evaluationsanforderungen, die erlauben festzustellen, ob die ST als Darlegung der EVG-Anforderungen geeignet sind. Explizit dargelegte Anforderungen sind in der Familie ASE_SRE enthalten.

- Die Familie **explizit dargelegte IT-Sicherheitsanforderungen (ASE_SRE)** umfasst Anforderungen an die Evaluation, die erlauben festzustellen, dass die explizit dargelegten Anforderungen klar und eindeutig ausgedrückt sind.

- Die **EVG-Übersichtsspezifikation (ASE_TSS)** gibt eine Definition der Sicherheitsfunktionen auf hoher Ebene, für die festgelegt wurde, dass sie die funktionalen Anforderungen erfüllen. Außerdem definiert sie Vertrauenswürdigkeitsmaßnahmen zur Erfüllung der Anforderungen an die Vertrauenswürdigkeit.

3.4.3 Konfigurationsmanagement

Die Klasse Konfigurationsmanagement (Configuration Management) wird mit dem Kürzel **ACM** bezeichnet. Sie definiert, dass der Hersteller für den EVG ein dokumentiertes und eventuell auch automatisiertes Konfigurationskontrollsystem einsetzen muss, um die Integrität des EVG zu erhalten. Weiterhin werden Verhinderungsmechanismen von nicht-autorisierten Modifizierungen, Hinzufügungen und Löschungen im EVG aufgezeigt. Die Klasse ACM enthält drei Familien:

- Die **CM-Automatisierung (ACM_AUT)** legt den Automatisierungsgrad fest, der bei der Kontrolle der Konfigurationsteile angewendet wird.

- Das **CM-Leistungsvermögen (ACM_CAP)** definiert die Eigenschaften des Konfigurationsmanagementsystems.

- Der **CM-Anwendungsbereich (ACM_SCP)** zeigt die EVG-Bestandteile auf, die vom Konfigurationsmanagementsystem kontrolliert werden müssen.

3.4.4 Auslieferung und Betrieb

Die Klasse Auslieferung und Betrieb (Delivery Operation) wird mit dem Kürzel **ADO** bezeichnet. Sie enthält Anforderungen zur Fehlerbehebung, die sich auf die Zeit nach Abschluss der Evaluation beziehen. Daher sind ihre Komponenten in keinem EAL enthalten, können aber als Ergänzung zur EAL gesehen und genutzt werden. Einzige Ausnahme sind die Komponenten der Familie ADO_IGS, die Bestandteil der EAL sind.

Außerdem werden Anforderungen an die Maßnahmen, Prozeduren und Normen, die sich mit der Sicherheit der Auslieferung, der Installation und des Betriebs des EVG befassen definiert. Sie sollen sicherstellen, dass der vom EVG gebotene Sicherheitsschutz während Transport, Installation, Anlauf und Betrieb nicht unterlaufen wird.

- Die **Auslieferung (ADO_DEL)** umfasst die Prozeduren und Operationen zur Erhaltung der Sicherheit während des Transports des EVG zum Benutzer.

- Die Familie **Installation, Generierung und Anlauf (ADO_IGS)** erfordert, dass die EVG-Kopie vom Systemverwalter so konfiguriert und aktiviert wird, dass sie die gleichen Schutzeigenschaften wie die EVG-Masterkopie aufweist.

3.4.5 Entwicklung

Die Klasse Entwicklung (Development) wird mit dem Kürzel **ADV** bezeichnet. Sie dient dazu, Anforderungen für die Umsetzung aller Sicherheitsfunktionen von einer hohen Spezifikationsebene bis hin zur Implementierung bereitzustellen. Jede Darstellung einer EVG-Sicherheitsfunktion liefert Informationen, die dem Evaluator helfen festzustellen, ob die funktionalen Anforderungen des EVG erfüllt sind.

- Die **Funktionale Spezifikation (ADV_FSP)** beschreibt die EVG-Sicherheitsfunktionen und muss eine vollständige und getreue Umsetzung der Sicherheitsanforderungen an den EVG sein. Außerdem sind auch Details zur externen Schnittstelle zum EVG enthalten.

- Der **Entwurf auf hoher Ebene (ADV_HLD)** ist eine Entwurfsspezifikation auf höchster Stufe, die die funktionale Spezifikation der EVG-Sicherheitsfunktionen in die Hauptbestandteile der EVG-Sicherheitsfunktionen verfeinert und die Grundstruktur der EVG-Sicherheitsfunktionen und der wichtigsten Hardware-, Firmware- und Softwareelemente angibt.

- Die **Darstellung der Implementierung (ADV_IMP)** ist die am wenigsten abstrakte Darstellung der EVG-Sicherheitsfunktionen, die die Details ihrer internen Arbeitsweise in der Form von Quellcode und Hardwarekonstruktionszeichnungen beschreibt.

- Die **Interna der EVG-Sicherheitsfunktionen (ADV_INT)** spezifizieren die erforderliche interne Strukturierung der EVG-Sicherheitsfunktionen.

- Der **Entwurf auf niedriger Ebene (ADV_LLD)** ist eine Entwurfsspezifikation, die den Entwurf auf hoher Ebene bis auf einen Detaillierungsgrad verfeinert, der als Grundlage zur Programmierung und/oder Hardwarekonstruktion dienen kann.

- Die **Übereinstimmung der Darstellung (ADV_RCR)** ist ein Nachweis der Übereinstimmung zwischen allen benachbarten Paaren verfügbarer EVG-Sicherheitsfunktionsdarstellungen, angefangen bei der EVG-Übersichtsspezifikation

bis zur am wenigsten abstrakten der bereitgestellten EVG-Sicherheitsfunktionsdarstellungen.

- Das **Sicherheitsmodell (ADV_SPM)** ist eine strukturierte Darstellung der Sicherheitspolitiken der EVG-Sicherheitsfunktionen, damit die funktionale Spezifikation mit den Sicherheitspolitiken der EVG-Sicherheitsfunktionen und schließlich mit den funktionalen Anforderungen an den EVG übereinstimmt. Erreicht wird dies durch entsprechende Übereinstimmungen zwischen der funktionalen Spezifikation, dem Sicherheitsmodell und den Sicherheitspolitiken, die im Modell dargestellt sind.

3.4.6 Handbücher

Die Klasse Handbücher (Guidance Documents) wird mit dem Kürzel **AGD** bezeichnet. Sie enthält die zwei Familien "Systemverwalterhandbuch" und "Benutzerhandbuch" und definiert Anforderungen, die die Verständlichkeit, Abdeckung und Vollständigkeit der vom Entwickler bereitgestellten Betriebsdokumentation betreffen.

- Das **Systemverwalterhandbuch (AGD_ADM)** beschreibt Anforderungen, die helfen sicherzustellen, dass Systemverwalter und Operatoren des EVG die umgebungsrelevanten Beschränkungen verstehen können. Es ist für den Entwickler das Medium, dem Systemverwalter detaillierte Informationen zur sicheren Verwaltung des EVG und zum wirksamen Gebrauch der EVG-Sicherheitsfunktionsprivilegien bereitzustellen.

- Das **Benutzerhandbuch (AGD_USR)** definiert Anforderungen, damit die Benutzer fähig sind, den EVG sicher bedienen zu können. Es ist für den Entwickler das Hauptmittel, dem EVG-Benutzer die notwendigen Hintergrundinformationen und spezielle Informationen zum korrekten Gebrauch der EVG-Schutzfunktionen bereitzustellen.

3.4.7 Lebenszyklus-Unterstützung

Die Klasse Lebenszyklus-Unterstützung (Lifecycle Support) wird mit dem Kürzel **ALC** bezeichnet. Sie beschreibt die Verwendung eines Lebenszyklus-Modells für alle Schritte der EVG-Entwicklung, einschließlich Fehlerbehebungsprozeduren und –politiken. Durch den korrekten Gebrauch von Werkzeugen und Techniken und der zum Schutz der Entwicklungsumgebung angewendeten Sicherheitsmaßnahmen erhöht sich die Vertrauenswürdigkeit.

- Die **Sicherheit bei der Entwicklung (ALC_DVS)** deckt die materiellen, organisatorischen, personellen und andere in der Entwicklungsumgebung ergriffene Sicherheitsmaßnahmen ab. Sie beschreibt darüber hinaus die materielle Sicherheit des Entwicklungsorts und die Kontrollen bei der Auswahl und Einstellung des Entwicklungspersonals.

- Die **Fehlerbehebung (ALC_FLR)** enthält Anforderungen zur Fehlerbeseitigung. Sie stellt sicher, dass vom EVG-Anwender entdeckte Fehler aufgezeichnet und korrigiert werden. Ihre Komponenten sind allerdings in keinem EAL enthalten, da sie sich auf die Zeit nach Abschluss der Evaluation beziehen.

- Die **Lebenszyklus-Beschreibung (ALC_LCD)** befasst sich mit den technischen Verfahren, die der Entwickler zur Produktion des Evaluationsgegenstandes einhalten muss.

- Die Familie **Werkzeuge und Techniken (ALC_TAT)** definiert die für die Analyse und Implementierung des EVG verwendeten Entwicklungswerkzeuge und enthält Anforderungen an diese.

3.4.8 Testen

Die Klasse Testen (Tests) wird mit dem Kürzel **ATE** bezeichnet. Sie fasst das Nachvollziehen der Herstellertests und die unabhängigen Korrektheitstests der Herstellerangaben durch den Evaluator zusammen.

- Die **Testabdeckung (ATE_COV)** behandelt die Vollständigkeit der funktionalen Tests und befasst sich mit dem Grad, bis zu dem die EVG-Sicherheitsfunktionen getestet sind.

- Die **Testtiefe (ATE_DPT)** befasst sich mit dem Detaillierungsgrad, bis zu dem getestet wird.

- Die Familie **Funktionale Tests (ATE_FUN)** ermittelt, ob die EVG-Sicherheitsfunktionen die Eigenschaften aufweisen, die zur Erfüllung der in deren ST enthaltenen Anforderungen notwendig sind.

- Die Familie **Unabhängiges Testen (ATE_IND)** spezifiziert den Grad, bis zu dem das funktionale Testen unabhängig, das heißt von einer anderen Person als dem Entwickler, ausgeführt werden muss.

3.4.9 Schwachstellenbewertung

Die Klasse Schwachstellenbewertung (Vulnerability Assessment) wird mit dem Kürzel **AVA** bezeichnet. Sie definiert Anforderungen an die Identifikation von Schwachstellen, die insbesondere bei Konstruktion, Betrieb, Missbrauch oder falscher Konfiguration des EVG entstehen.

- Die **Analyse der verdeckten Kanäle (AVA_CCA)** zielt auf die Entdeckung und Analyse unerwünschter Kommunikationskanäle ab, die zur Verletzung der vorgesehenen EVG-Sicherheitsfunktionen ausgenutzt werden können. Verdeckte Kanäle sind nur dann relevant, wenn in den Sicherheitsvorgaben eine Informationsflusskontrollstrategie verwendet wird.

- Die Familie **Missbrauch (AVA_MSU)** untersucht, ob es einem Systemverwalter oder Benutzer, der mit den Handbüchern vertraut ist, möglich ist festzustellen, ob Konfiguration und Betrieb des EVG unsicher sind.

- Die **Stärke der EVG-Sicherheitsfunktionen (AVA_SOF)** bezieht sich auf EVG-Sicherheitsfunktionen, die Wahrscheinlichkeits- oder Permutationsmechanismen einsetzen, denn selbst wenn solche Funktionen nicht umgangen, deaktiviert oder verfälscht werden können, besteht doch die Möglichkeit, dass diese durch einen direkten Angriff außer Kraft gesetzt werden. Jede solche EVG-Sicherheitsfunktion kann anhand ihrer Stärke eingeordnet werden.

- Die **Schwachstellenanalyse (AVA_VLA)** deckt die Identifikation von Konstruktionsschwachstellen und operationelle Schwachstellen ab.

3.4.10 Erhaltung der Vertrauenswürdigkeit

Die Klasse Erhaltung der Vertrauenswürdigkeit (Maintenance of Assurance) wird mit dem Kürzel **AMA** bezeichnet. Sie beruht auf den anderen oben definierten Klassen und dient der Erhaltung des Grad der Vertrauenswürdigkeit, damit der EVG seine Sicherheitsvorgaben nach Änderungen am EVG oder an seiner Umgebung auch weiterhin erfüllt.

- Der **Plan zur Erhaltung der Vertrauenswürdigkeit (AMA_AMP)** legt den Plan und die Prozeduren fest, die ein Entwickler implementieren muss, um sicherzustellen, dass die für den evaluierten EVG ermittelte Vertrauenswürdigkeit nach Änderungen am EVG oder seiner Umgebung weiterhin erhalten bleibt.

- Der **Kategorisierungsbericht der EVG-Komponenten (AMA_CAT)** enthält eine Kategorisierung der EVG-Komponenten anhand ihrer Relevanz für die Sicherheit. Diese Kategorisierung ist entscheidend für die Zielrichtung der Sicherheitsauswirkungsanalyse des Entwicklers.

- Der **Nachweis der Erhaltung der Vertrauenswürdigkeit (AMA_EVD)** beruht auf dem Plan zur Erhaltung der Vertrauenswürdigkeit und soll Vertrauen schaffen, dass die Vertrauenswürdigkeit des EVG erhalten wird.

- Die **Sicherheitsauswirkungsanalyse (AMA_SIA)** zielt auf die Schaffung von Vertrauen ab, dass die Vertrauenswürdigkeit des EVG erhalten geblieben ist. Dies geschieht durch eine Analyse der Sicherheitsauswirkungen aller Änderungen mit Einfluss auf den EVG, seit dessen Prüfung und Bewertung. Diese Analyse muss vom Entwickler durchgeführt werden.

4. Die Evaluation auf der Basis von Common Criteria

Im folgenden Kapitel wird beschrieben, wie eine Sicherheitsevaluierung ablaufen soll, was und wie untersucht wird und was sie leisten bzw. nicht leisten kann. Dabei wird der Ablauf des Zertifizierungsprozesses in seinen grundsätzlichen Schritten dargelegt, beginnend bei der Antragstellung bis hin zur Erteilung des Zertifikates.

Ein entscheidender Faktor für das Verständnis der Evaluation nach CC ist, sich deutlich zu machen, dass die Sicherheitsfunktionalität vom Hersteller beschrieben und ihr Vorhandensein vom Evaluator geprüft wird. Es können also nur vorher spezifizierte Funktionalitäten überprüft werden.

Die Grundlagen für die Evaluation bilden vor allem die Sicherheitsvorgaben und die Produktdokumentation. Dabei können die Sicherheitsvorgaben auf einem Schutzprofil basieren und die geforderte Vertrauenswürdigkeitsstufe enthalten. Die Anforderungen an die Prüfung und Bewertung von Schutzprofilen, Sicherheitsvorgaben, Produktdokumentation und das Testen sind in Vertrauenswürdigkeitsklassen festgelegt.

4.1 Die Vorbereitung

Die Vorbereitung ist entscheidend für das Gelingen und den Aufwand der Evaluation, da nicht beachtete Aspekte in der Vorbereitung eine Reihe von Fehlern nach sich ziehen können, die den Erfolg der Zertifizierung eventuell beeinträchtigen.

Schon zu Beginn der Entwicklung eines IT-Produkts sollte sich der Hersteller überlegen, welche Vertrauenswürdigkeitsstufe er für sein Produkt beantragen möchte. Denn die Auswahl der Vertrauenswürdigkeitsstufe ist eine wichtige Grundlage für die spätere Evaluation. Die Auswahl beruht im Wesentlichen auf dem geplanten Verwendungszweck des Produkts, wobei unterschiedliche, sich gegenseitig beeinflussende Aspekte berücksichtigt werden müssen. Der normalerweise wichtigste Aspekt ist die Erhöhung der Vertrauenswürdigkeit in die Funktionalität des Produkts. Ebenfalls entscheidend ist die unabhängige Bestätigung der Produktqualität. Außerdem können auch rechtliche und organisatorische Vorschriften wie das SigG auf die Auswahl einer Vertrauenswürdigkeitsstufe Einfluss haben. Nicht zu unterschätzen ist im Übrigen auch der Kostenaspekt und der Werbeeffekt, die normalerweise beide bei einer hohen Vertrauenswürdigkeitsstufe erheblich größer sein werden, als bei einer niedrigeren. Die Entscheidung welche Vertrauenswürdigkeitsstufe angepeilt werden soll, hängt also unter anderem von folgenden Faktoren ab:

- Verwendungszweck
- Funktionalität des Produkts
- Bestätigung der Produktqualität
- Rechtliche und organisatorische Vorschriften
- Kostenaspekte
- Werbeeffekte
- Art des Entwicklungsprozesses
- Verfügbaren Ressourcen beim Hersteller

Fallen rechtliche und organisatorische Aspekte weg, dann kann der Hersteller des IT-Produkts frei die angestrebte Vertrauenswürdigkeitsstufe wählen, die zertifiziert werden soll. Ist dies geschehen, dann muss ein Kosten- und Zeitplan der Evaluation bis hin zur endgültigen Zertifizierung aufgestellt werden. Diese Pläne sind abhängig von der Testtiefe und dem Umfang der zu testenden Sicherheitsfunktionen.

„Mit steigender Evaluierungsstufe nehmen der Umfang und der Detaillierungsgrad der zu evaluierenden Produkt- und Design-Dokumentation und dementsprechend auch die Prüftiefe und der Testumfang zu. Wird z. B. bei der Stufe EAL3 noch auf einen Entwurf auf niedriger Ebene (Feinentwurf) und die Darstellung der Implementierung (Quellcode oder Hardwarekonstruktionszeichnungen) verzichtet, so müssen diese Design-Dokumente ab der Stufe EAL4 in die Evaluierung einbezogen werden. In höheren Stufen werden darüber hinaus ein formales Sicherheitsmodell und Design-Dokumentation in semiformaler oder formaler Darstellung gefordert." [17)]

„Die Philosophie der CC besagt und die Erfahrung zeigt, dass höhere Vertrauenswürdigkeit die Folge eines höheren Evaluationsaufwandes ist, und dass das Ziel der Zertifizierung dann besteht, mit minimalem Aufwand den erforderten Grad an Vertrauenswürdigkeit zu erzielen." [12)]

Das BSI hat übrigens einen Leitfaden über die IT Sicherheit auf Basis der CC herausgegeben, in dem eine interessante Übersicht über schon bewertete Produkte mit ihrer EAL Stufe aufgeführt ist. Die Übersicht kann bei der Auswahl der Vertrauenswürdigkeitsstufe helfen, indem der Hersteller eine Vorstellung über die Konkurrenzprodukte derselben Produktkategorie bekommt.

Bevor nun der Evaluations- und Zertifizierungsprozess erläutert wird, ist es sinnvoll, nochmals auf einige Aufgaben aufmerksam zu machen, die bei der Erstellung des Schutzprofils, der Sicherheitsvorgaben und der Produktdokumentation beachtet werden sollten.

- Das **Schutzprofil** ist eine implementierungsunabhängige Menge von IT-Sicherheitsanforderungen und ein beschreibendes Dokument mit den Themen Einführung, EVG-Beschreibung, EVG-Sicherheitsumgebung, Sicherheitsziele, IT-Sicherheitsanforderungen, Anwendungsbemerkungen und Erklärung. Es soll durch die Evaluierung als vollständig, konsistent und technisch verträglich bestätigt werden, damit es als Grundlage der Entwicklung von Sicherheitsvorgaben verwendet werden kann.

- Die **Sicherheitsvorgaben** enthalten IT-Sicherheitsanforderungen, mit denen die Sicherheitsfunktionen und die Sicherheitsmaßnahmen der Vertrauenswürdigkeit festgelegt werden. In der Einführung soll der EVG und seine Sicherheitsfunktionen identifiziert und grafisch dargestellt werden. Danach wird der EVG hinsichtlich seiner Sicherheitsanforderungen an den Produkt- oder Systemtyp beschrieben, sowie die EVG-Sicherheitsumgebung und der erwartete Gebrauch dargelegt. Eine Aufführung der Annahmen über die Sicherheitsaspekte soll im Anschluss folgen, damit die Anzahl der potentiellen Bedrohungen eingeschränkt werden kann. Auch die Bedrohungen und die Sicherheitspolitiken müssen explizit beschrieben werden. Es soll ein Kapitel über

die Sicherheitsziele und eines über die funktionalen Komponenten des EVG, sowie die Anforderungen an die Vertrauenswürdigkeit folgen, bevor schließlich die EVG-Übersichtsspezifikation und die PP-Postulate beschrieben werden. Zuletzt sollte noch eine Erklärung abgegeben werden, die den Nachweis zur Prüfung und Bewertung der Sicherheitsvorgaben darstellt.

- Die **Produktdokumentation** besteht zum einen aus der Gesamtheit der dokumentierten Sicherheitsfunktionen und zum anderen aus der Dokumentation der Anforderungen an die Vertrauenswürdigkeitsklassen.

4.2 Der Evaluations- und Zertifizierungsprozess

Das Schutzprofil ist zwar nicht unbedingt nötig, aber wenn es vorhanden ist, bildet es die Grundlage der Sicherheitsvorgaben und der Evaluation. Es reduziert außerdem den Arbeitsaufwand und damit auch die Kosten. Darüber hinaus wird mit dem Schutzprofil eine Vergleichsgrundlage für alle Produkte, die nach demselben Schutzprofil bewertet werden, geschaffen. Zu Beginn des Evaluierungsprozesses findet die Prüfung des Schutzprofils statt. Danach folgt die Evaluierung der Sicherheitsvorgaben, die von der Zertifizierungsstelle erfolgreich abgenommen werden muss, bevor die eigentliche Evaluierung des EVG stattfindet. Während der Evaluation wird ein Evaluationsbericht von der Evaluationsstelle erstellt und die Zertifizierungsstelle überprüft die einheitliche Vorgehensweise auf Basis einer Evaluationsmethodologie. Wird der Evaluationsbericht erfolgreich abgenommen, endet die Evaluierung. Im Falle einer erfolgreichen Evaluation erstellt dann die Zertifizierungsstelle einen Zertifizierungsreport, der letztendlich zum Zertifikat führt und veröffentlicht ihn, falls gewünscht.

Alle Phasen der Zertifizierung sollten unter direkter Beteiligung des Herstellers des IT-Produkts durchgeführt werden, um die Effizienz des Evaluations- und Zertifizierungsprozess zu erhöhen. Zu Beginn werden gemeinsam von Hersteller, Evaluationsstelle und Zertifizierungsstelle die Meilensteine festgelegt. Damit weiß jede beteiligte Stelle über den Ablauf der Evaluation Bescheid und kann bei Unklarheiten über die Ergebnisse einer Einzelprüfung oder deren Interpretation eine gemeinsame Aufklärungssitzung veranlassen. Falls nötig, können dann Meilensteine verschoben werden und Nachbesserungen am Produkt oder an der Dokumentation vorgenommen werden. Durch die Einbeziehung aller Beteiligten an dem Evaluationsprozess können mögliche Probleme schneller mitgeteilt und gelöst werden.

Wie schon erwähnt, wird für ein einheitliches Vorgehen bei einer Evaluation neben den Common Criteria auch eine Evaluationsmethodologie benötigt, in der das Vorgehen beschrieben und definiert ist. Hinzu kommen spezifische Vorgaben an den juristischen und verwaltungstechnischen Rahmen einer Evaluation, die als Evaluationsschema oder auch Zertifizierungsschema bezeichnet werden. Folgende Grafik verdeutlicht diesen Zusammenhang:

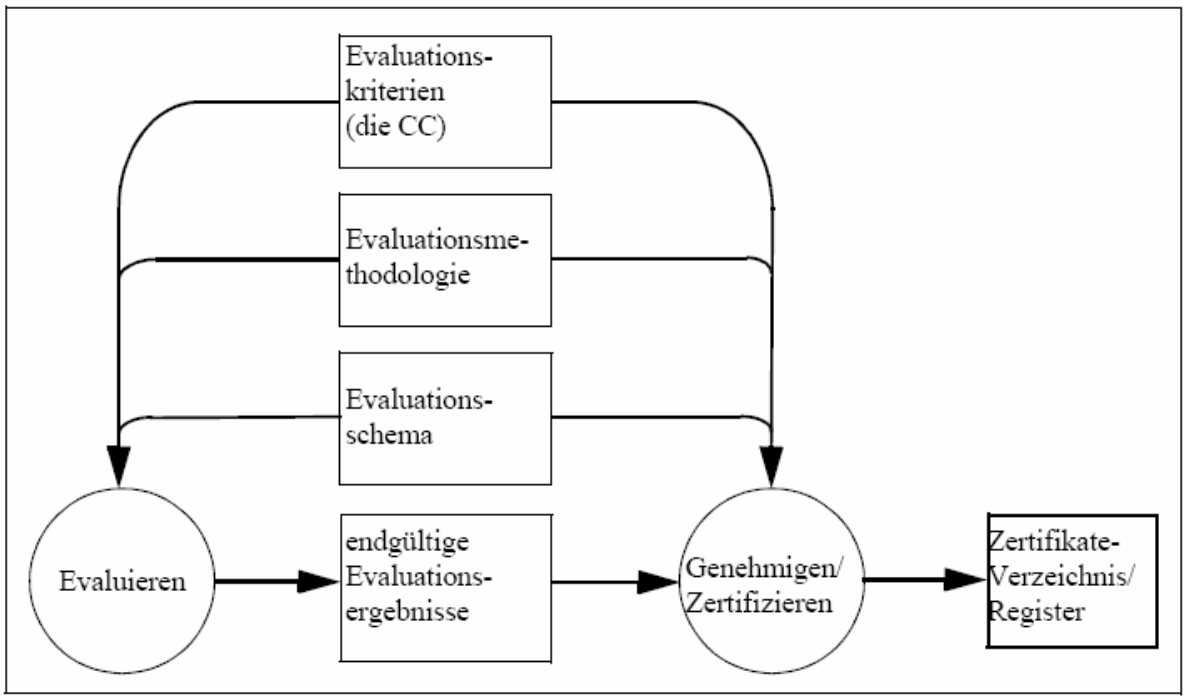


Abbildung 16

An dieser Stelle bietet es sich an, dass man sich in die Evaluationsmethodologie (CEM) einarbeitet, um den Zertifizierungsprozess noch besser nachvollziehen zu können. Hier wird darauf verzichtet, da der Umfang den Rahmen dieser Arbeit sprengen würde. Im Folgenden wird dafür auf ein Evaluationsschema/Zertifizierungsschema näher eingegangen.

4.3 Das Zertifizierungsschema DIN 45001 (BSI & CC)

Jede Nation besitzt normalerweise ein eigenes Zertifizierungsschema auf Basis von CC. Abgestimmt zwischen den an der Erstellung von CC beteiligten Staaten und Organisationen ist aber, dass jedes nationale Schema zu gleichwertigen Ergebnissen führt. In Deutschland ist das Schema des BSI durch das Deutsche Institut für Normung (DIN) in der Norm DIN 45001 geregelt. Es gibt aber in Deutschland noch weitere Zertifizierungsstellen mit eigenen Schemata, die vertraglich festgelegt haben, auch die Evaluationsergebnisse der anderen Stellen anzuerkennen. Da die BSI aber direkt an der Erstellung von CC beteiligt ist, wird dieses Schema hier stellvertretend für alle anderen Schemata behandelt.

Das Zertifizierungsschema kann in fünf Phasen unterteilt werden:

- Vorphase und Logistik
- Evaluierung
- Zertifizierung
- Weitere Hilfestellung
- Re-Zertifizierung

Noch vor Beginn der **Vorphase** findet im Regelfall eine Beratung des Antragstellers durch die Prüfstelle und die Zertifizierungsstelle statt. Dann folgt in der Vorphase die Erarbeitung von Sicherheitsvorgaben und Meilensteinen für die Evaluation. Ist dies abgeschlossen, so erfolgt zwischen der Prüfstelle und dem Antragsteller der Abschluss eines Evaluierungsvertrags. Danach wird bei der Zertifizierungsstelle, die in diesem Fall das BSI ist, ein Zertifizierungsantrag gestellt. Es folgt die Benennung von so genannten Prüfbegleitern und der Antragsteller stellt das Produkt mit der notwendigen Dokumentation zur Verfügung.

Der nächste Schritt ist der Beginn der **Evaluierung** des Produkts durch die Prüfstelle. Sie dokumentiert und begründet die Ergebnisse der Prüfungen in Prüfberichten. Während dieses Prüfprozesses begleitet die Zertifizierungsstelle die Evaluation, um die einheitlichen Standards der Vorgehensweise und Methodik zu wahren und zu prüfen. Außerdem stellt sie sicher, dass vergleichbare Bewertungen erstellt werden. Die Evaluation wird mit der Erstellung des Evaluierungsberichts durch die Prüfstelle, dessen Abnahme durch die Zertifizierungsstelle und die Übergabe an den Antragsteller abgeschlossen.

In der Phase der **Zertifizierung** wird von der Zertifizierungsstelle der Zertifizierungsreport erstellt und ein Zertifizierungsbescheid für den Antragsteller ausgestellt. Wenn dieser zustimmt, werden die Ergebnisse der Evaluation veröffentlicht.

Weitere Hilfestellung gibt die Zertifizierungsstelle anschließend dem Antragsteller in Bezug auf eine mögliche Re-Zertifizierung neuer Versionen des Produkts. Außerdem bietet die Zertifizierungsstelle Unterstützung bei einer Veröffentlichung und Verteilung des Zertifizierungsreports an.

In einer **Re-Zertifizierung** neuer Versionen des Produkts kann auf die vorangegangenen Ergebnisse der Zertifizierung zurückgegriffen und darauf aufgebaut werden. Eine Re-Zertifizierung sollte daher einen erheblich geringeren Aufwand haben, als die ursprüngliche Zertifizierung.

4.4 Die EAL-Stufen

Die CC bestehen aus mehreren Evaluierungsstufen für die Vertrauenswürdigkeit, auf denen Produkte bewertet werden. Innerhalb der CC werden diese Stufen als Evaluation Assurance Level (EAL) bezeichnet. Dabei ist EAL-1 die niedrigste und EAL-7 die höchste Stufe der Vertrauenswürdigkeit. Die hierarchische Anordnung besagt dabei, dass jede höhere EAL-Stufe die niedrigeren beinhaltet.

„Typische kommerzielle Systeme können maximal die vierte Stufe der EAL-Zertifizierung erreichen. Die drei nächsthöheren EAL-Stufen 5 bis 7 sind solchen Produkten vorbehalten, die bereits eigens mit Sicherheitstechniken entwickelt wurden.“ [4)]

Die Vorgehensweise der CC hat das Ziel, die verschiedenen Konzepte der Vertrauenswürdigkeit und der Erhaltung dieser Vertrauenswürdigkeit während des Betriebs des EVG zu identifizieren. Dazu werden je nach EAL-Stufe andere Vertrauenswürdigkeitsanforderungen benötigt wie zum Beispiel die zunehmende

Schärfe, der größere Anwendungsbereich und/oder die zunehmende Testtiefe. Es können aber auch ganz neue Anforderungen hinzugefügt werden. Jede EAL umfasst aber nicht mehr als eine Komponente einer Vertrauenswürdigkeitsfamilie. Das heißt, dass in einer Familie unterschiedliche Komponenten für die jeweilige EAL Stufe existieren. Darüber hinaus werden in der EAL alle Vertrauenswürdigkeitsabhängigkeiten jeder Komponente erfüllt. Es folgt eine Übersicht über die EAL-Stufen und ihre Anforderungen:

EAL- Stufe	Anforderungen
EAL-0	unzulängliche Vertrauenswürdigkeit
EAL-1	funktionell getestet
EAL-2	strukturell getestet
EAL-3	methodisch getestet und überprüft
EAL-4	methodisch entwickelt, getestet und durchgesehen
EAL-5	semiformal entworfen und getestet
EAL-6	semiformal verifizierter Entwurf, getestet
EAL-7	formal verifizierter Entwurf, getestet

Tabelle 3

Beginnend mit EAL-1 werden nun alle ihr folgenden EAL-Stufen genauer erläutert.

Die **EAL-1** bietet durch die Analyse der Sicherheitsfunktionen unter Verwendung einer funktionalen und einer Schnittstellenspezifikation sowie von Handbüchern eine Grundstufe an Vertrauenswürdigkeit. Dadurch soll das Sicherheitsverhalten verstanden werden. Die Analyse wird durch unabhängiges Testen der EVG-Sicherheitsfunktionen unterstützt.

„EAL1 ist anwendbar, wenn ein gewisses Maß an Vertrauen in einen korrekten Betrieb erforderlich ist, die Bedrohungen der Sicherheit aber nicht als ernst angesehen werden. Sie wird dort von Bedeutung sein, wo unabhängige Vertrauenswürdigkeit benötigt wird, um die Behauptung zu unterstützen, daß dem Schutz persönlicher oder vergleichbarer Informationen angemessene Aufmerksamkeit gewidmet wurde.“ [13)]

Die **EAL-2** schafft Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen Spezifikation und einer Schnittstellenspezifikation sowie von Handbüchern und des Entwurfs des EVG auf hoher Ebene analysiert werden, um das Sicherheitsverhalten nachzuvollziehen. Unterstützt wird die Analyse durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation durch selektive,

unabhängige Bestätigung der Entwicklertestergebnisse, durch Analyse der Stärke der Funktion und durch einen Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen. Die EAL-2 schafft Vertrauenswürdigkeit auch mittels eines Konfigurationsverzeichnisses für den EVG und durch einen Nachweis der Sicherheit der Auslieferungsprozeduren.

„EAL2 erfordert die Kooperation des Entwicklers hinsichtlich der Lieferung von Entwurfsinformationen und Testergebnissen. Dabei sollte aber der dem Entwickler abgeforderte Arbeitsaufwand das in gut geführten Betrieben übliche Maß nicht überschreiten. Das heißt, sie soll keine erheblichen finanziellen oder zeitlichen Zusatzinvestitionen erfordern.“ [13)]

Die **EAL-3** bietet Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen Spezifikation und einer Schnittstellenspezifikation sowie von Handbüchern und des Entwurfs des EVG auf hoher Ebene analysiert werden, um das Sicherheitsverhalten zu verstehen. Unterstützt wird die Analyse durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des Entwurfs auf hoher Ebene, durch selektive, unabhängige Bestätigung der Entwicklertestergebnisse, durch Analyse der Stärke der Funktion und durch einen Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen. Die EAL-3 schafft Vertrauenswürdigkeit auch durch Kontrollen der Entwicklungsumgebung, durch ein EVG-Konfigurationsmanagement und den Nachweis der Sicherheit der Auslieferungsprozeduren.

„EAL3 erlaubt einem gewissenhaften Entwickler, durch positive technische Sicherheitsmaßnahmen auf der Entwicklungsstufe maximale Vertrauenswürdigkeit zu erzielen, ohne die bestehenden, stimmigen Entwicklungspraktiken wesentlich zu verändern.“ [13)]

Die **EAL-4** schafft Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen Spezifikation und einer vollständigen Schnittstellenspezifikation, von Handbüchern, des EVG-Entwurfs auf hoher Ebene und auf niedriger Ebene sowie einer Teilmenge der Implementierung analysiert werden, um das Sicherheitsverhalten zu verstehen. Vertrauenswürdigkeit wird darüber hinaus auch durch ein informelles Modell der EVG-Sicherheitspolitik erzielt. Unterstützt wird die Analyse durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des Entwurfs auf hoher Ebene, durch selektive, unabhängige Bestätigung der Entwicklertestergebnisse, durch die Analyse der Stärke der Funktion und durch einen Nachweis der Suche des Entwicklers nach Schwachstellen und durch eine unabhängige Schwachstellenanalyse, welche die Widerstandsfähigkeit gegen Angreifer mit einem niedrigen Angriffspotential nachweist. Die EAL-4 schafft Vertrauenswürdigkeit auch durch Kontrollen der Entwicklungsumgebung und zusätzliches EVG-Konfigurationsmanagement einschließlich Automatisierung sowie Nachweis der Sicherheit der Auslieferungsprozeduren.

„EAL4 erlaubt einem Entwickler, durch positive technische Sicherheitsmaßnahmen maximale Vertrauenswürdigkeit zu erzielen, basierend auf bewährten betrieblichen Entwicklungspraktiken, die zwar scharf sind, aber keine tiefgehenden Spezialkenntnisse, Fähigkeiten oder andere Betriebsmittel erfordern. EAL4 ist die höchste Stufe, bei der eine Nachrüstung einer Produktreihe wahrscheinlich noch wirtschaftlich durchführbar ist.“ 13)

Die **EAL-5** bietet Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen Spezifikation und einer vollständigen Schnittstellenspezifikation, von Handbüchern, des EVG-Entwurfs auf hoher und niedriger Ebene und der gesamten Implementierung analysiert werden, um das Sicherheitsverhalten zu verstehen. Vertrauenswürdigkeit wird auch durch ein formales Modell der EVG-Sicherheitspolitik und eine semiformale Darstellung der funktionalen Spezifikation und des Entwurfs auf hoher Ebene sowie einen semiformalen Nachweis der Übereinstimmung untereinander erzielt. Ebenfalls verlangt wird ein modularer EVG-Entwurf. Die Analyse wird unterstützt durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des Entwurfs auf hoher und auf niedriger Ebene, durch die selektive, unabhängige Bestätigung der Entwicklertests, durch die Analyse der Stärke der Funktion und den Nachweis der Suche des Entwicklers nach Schwachstellen und durch eine unabhängige Schwachstellenanalyse, die den Widerstand gegen Angreifer mit einem mittleren Angriffspotential nachweist. Die Analyse umfasst ebenso die Validierung der Entwickleranalyse der verdeckten Kanäle. Die EAL-5 schafft Vertrauenswürdigkeit auch durch Kontrollen der Entwicklungsumgebung, ein umfassendes EVG-Konfigurationsmanagement einschließlich Automatisierung sowie Nachweis der Sicherheit der Auslieferungsprozeduren.

„EAL5 erlaubt einem Entwickler, maximale Vertrauenswürdigkeit durch technische Sicherheitsmaßnahmen zu erzielen, basierend auf scharfen betrieblichen Entwicklungspraktiken, die durch begrenzten Einsatz von Sicherheits-Spezialtechniken zur Entwicklung unterstützt werden. Ein solcher TOE (EVG) ist wahrscheinlich mit der Absicht entworfen und entwickelt, die Vertrauenswürdigkeit der Stufe EAL5 zu erreichen. Es ist wahrscheinlich, daß die durch die EAL5-Anforderungen verursachten zusätzlichen Kosten, bezogen auf eine strikte Entwicklung ohne Anwendung von Spezialpraktiken, nicht erheblich sind.“ 13)

Die **EAL-6** schafft Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen Spezifikation und einer vollständigen Schnittstellenspezifikation, von Handbüchern, des EVG-Entwurfs auf hoher und niedriger Ebene und einer strukturierten Darstellung der Implementierung analysiert werden, um das Sicherheitsverhalten zu verstehen. Vertrauenswürdigkeit wird außerdem durch ein formales Modell der EVG-Sicherheitspolitik und eine semiformale Darstellung der funktionalen Spezifikation und des Entwurfs auf hoher Ebene und auf niedriger Ebene sowie einen semiformalen Nachweis der Übereinstimmung untereinander erzielt. Ein modularer und mehrschichtiger EVG-Entwurf wird ebenfalls verlangt. Die Analyse wird unterstützt durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des

Entwurfs auf hoher und auf niedriger Ebene, durch die selektive, unabhängige Bestätigung der Ergebnisse der Entwicklertests, durch die Analyse der Stärke der Funktion und den Nachweis der Suche des Entwicklers nach Schwachstellen und durch eine unabhängige Schwachstellenanalyse, die den Widerstand gegen Angreifer mit einem hohen Angriffspotential nachweist. Die Analyse umfasst ebenso die Validierung der systematischen Entwickleranalyse der verdeckten Kanäle. Die EAL-6 schafft Vertrauenswürdigkeit auch durch Anwendung eines strukturierten Entwicklungsverfahrens, Kontrollen der Entwicklungsumgebung, ein umfassendes EVG-Konfigurationsmanagement einschließlich vollständiger Automatisierung sowie Nachweis der Sicherheit der Auslieferungsprozeduren.

„EAL6 erlaubt den Entwicklern, durch Anwendung von Techniken zur Sicherheitsentwicklung in einer streng kontrollierten Entwicklungsumgebung eine hohe Vertrauenswürdigkeit zu erzielen, um einen erstklassigen TOE (EVG) zum Schutz hoher Werte gegen signifikante Risiken zu entwickeln. EAL6 ist daher anwendbar für die Entwicklung von Sicherheits-EVG zum Gebrauch in Situationen mit hohem Risiko, in denen die große Bedeutung der geschützten Werte die Zusatzkosten rechtfertigt.“ [13)]

Die **EAL-7** schafft Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen und einer vollständigen Schnittstellenspezifikation, von Handbüchern, des EVG-Entwurfs auf hoher und niedriger Ebene und einer strukturierten Darstellung der Implementierung analysiert werden, um das Sicherheitsverhalten zu verstehen. Vertrauenswürdigkeit wird außerdem durch ein formales Modell der EVG-Sicherheitspolitik, durch eine formale Darstellung der funktionalen Spezifikation und des Entwurfs auf hoher Ebene, durch eine semiformale Darstellung des Entwurfs auf niedriger Ebene sowie durch einen formalen und semiformalen Nachweis der Übereinstimmung untereinander , wie jeweils angemessen, erzielt. Ein modularer und mehrschichtiger und einfacher EVG-Entwurf wird ebenfalls verlangt. Die Analyse wird unterstützt durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des Entwurfs auf hoher und auf niedriger Ebene sowie der Darstellung der Implementierung, durch die vollständige, unabhängige Bestätigung der Ergebnisse der Entwicklertests, durch die Analyse der Stärke der Funktion und den Nachweis der Suche des Entwicklers nach Schwachstellen und durch eine unabhängige Schwachstellenanalyse, die den Widerstand gegen Angreifer mit einem hohen Angriffspotential nachweist. Die Analyse umfasst ebenso die Validierung der systematischen Entwickleranalyse der verdeckten Kanäle. Die EAL-7 schafft Vertrauenswürdigkeit auch durch Anwendung eines strukturierten Entwicklungsverfahrens, Kontrollen der Entwicklungsumgebung, ein umfassendes EVG-Konfigurationsmanagement einschließlich vollständiger Automatisierung sowie durch den Nachweis der Sicherheit der Auslieferungsprozeduren.

„EAL7 ist anwendbar für die Entwicklung von Sicherheits-EVG zur Anwendung in Situationen mit extrem hohem Risiko und/oder in Fällen, in denen die große Bedeutung der Werte die höheren Kosten rechtfertigt. Der praktische Einsatz von EAL7 ist gegenwärtig auf TOE (EVG) mit hochkonzentrierter Sicherheitsfunktionalität begrenzt, die sich für umfangreiche formale Analysen eignet.“ [13)]

Nachdem nun alle EAL-Stufen ausführlich dargelegt wurden, kann anhand der folgenden Übersicht exakt ausgelesen werden, welche Vertrauenswürdigkeitskomponente für die jeweilige Vertrauenswürdigkeitsstufe erfolgreich umgesetzt werden muss. Auf der linken Seite befinden sich die schon ausführlich besprochenen Vertrauenswürdigkeitsklassen aufgeteilt in die Vertrauenswürdigkeitsfamilien. Weiter rechts kann unter der jeweiligen EAL-Stufe die Komponente der Familie abgelesen werden. Anhand dieser Information kann in CC nachgeschlagen werden, welche Anforderungen für die Komponente erfüllt sein müssen, damit sie der EAL-Stufe genüge tut.

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitsfamilie	Vertrauenswürdigkeitskomponenten nach Vertrauenswürdigkeitsstufen						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Konfigurationsmanagement	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Auslieferung und Betrieb	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Entwicklung	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Handbücher	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Lebenszyklus-Unterstützung	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Testen	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Schwachstellenbewertung	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Abbildung 17

4.5 Die Kosten einer CC-Evaluierung

Eine Evaluierung auf Basis von CC ist natürlich auch mit finanziellen Kosten verbunden. Laut Corsec Security [28)] gilt es dabei vier Faktoren zu berücksichtigen, um eine Kostenanalyse aufstellen zu können:

1. Die Kosten eines Testlabors
2. Den Änderungsaufwand und die damit verbundenen Kosten, ein Produkt den gestellten Anforderungen entsprechen zu lassen
3. Die Aufbereitung von Vertrauenswürdigkeitsdokumenten in für die Evaluierung notwendige Teilpakete
4. Die Gebühren der Offiziellen Zertifizierungsstellen

Corsec Security sieht weitere wesentliche Faktoren in der EAL-Stufe, der Evaluationskomplexität eines Produktes und dem Status der schon vorhandenen Dokumentation, da die Dokumentation für CC selbst bei niedrigen EAL eine große Rolle spielt. Natürlich sind auch die internen Kosten, nicht zu vernachlässigen, da zum Beispiel eigene Entwickler für den Evaluationsprozess abgestellt werden müssen.

Die Kosten einer Zertifizierung sind also von vielen verschiedenen Faktoren abhängig und summieren sich leicht zu einem großen Betrag. Die Direktorin des NIAP, Jean Schaffer, nimmt zu den Kosten einer CC-Zertifizierung Stellung. „Critics say Common Criteria testing costs too much and takes too long, but Schaffer argued that these claims are made by those who do not have firsthand knowledge about the testing. Feedback from the labs shows that testing for Evaluation Assurance Level (EAL) 2 — the minimum level of security, which includes products such as firewalls, intrusion-detection systems, routers and switches — costs $100,000 to $170,000 and takes four to six months. The highest level of security — EAL 4, which includes operating systems that support peer-to-peer communications — costs $300,000 to $750,000 and takes one year to two years.“ [25)]

Die von Schaffer genannten Kosten müssen durch den Verkauf des evaluierten Produkts erst einmal wieder eingenommen werden, damit sich die Zertifizierung rechnen kann. Nicht jeder mittelständische IT-Betrieb wird sich eine Zertifizierung auf Basis von CC leisten können. Bei der Weiterentwicklung von CC sollen daher verstärkt wirtschaftliche Aspekte berücksichtigt werden, so Dr. Markus Mackenbrock vom BSI. [24)]

5. Ein Common Criteria Tool

Im Rahmen der Schaffung der CC haben sich die an der Erstellung beteiligten Stellen auch Gedanken über eine Toolunterstützung des Zertifizierungsprozesses gemacht. Allen voran hat das National Institute of Standards and Technology (NIST) den Schritt gewagt, ein Tool produzieren zu lassen. Im Rahmen der National Information Assurance Partnership (NIAP) Lizenzvereinbarung zwischen der National Security Agency (NSA) und der US Regierung wurde die Firma Sparta beauftragt, ein Tool zu produzieren. Das Ergebnis des Entwicklungsprozesses ist die CC Toolbox, die aus zwei Tools zur Erstellung von PPs und STs besteht. Darüber hinaus entstand die CC Profiling Knowledge Base (CCPKB), die die Grundlage der CC Toolbox darstellt und eine umfangreiche Dokumentation, die sich aus einem Benutzerhandbuch, einer Tour durch die CC Toolbox und einem Referenzhandbuch zusammensetzt. Die CC Toolbox ist ein Open Source Projekt und daher kostenlos und frei verfügbar.

5.1 Die CC Profiling Knowledge Base

Anhand der festen Zuordnung von Vertrauenswürdigkeitskomponenten zu den EAL-Stufen lässt sich genau identifizieren, welche Vertrauenswürdigkeitsfunktionen in einem IT-Produkt umgesetzt werden müssen. Dieser Prozess wird von der CC Toolbox unterstützt und je nach EAL-Stufe kann ein PP oder ST als Output generiert werden. Auch die Auswahl der Anforderungen an die Funktionalität kann durch die CC Toolbox gesteuert werden, da jede funktionale Familie über mindestens eine Komponente verfügt, die die Sicherheitsanforderungen an die konkrete Funktionalität beschreibt. Daher können mittels Verknüpfungstabellen, den so genannten Mappingtabellen, Zuordnungen zwischen Bedrohungen, Angriffen, Sicherheitszielen und den funktionalen Klassen gemacht werden. Des Weiteren sind auch Verknüpfungen mit Sicherheitspolitiken, Sicherheitsannahmen und einer selbst zu definierenden Systemumgebung möglich. Diese Verknüpfungen sind in der CCPKB beispielhaft für das US-Verteidigungsministerium vordefiniert und können auch selber festgelegt werden. Die folgende selbst erstellte Grafik verdeutlicht die oben genannten Zusammenhänge. Dabei Stellen die Knoten jeweils Tabellen in der CCPKB und die Verbindungslinien ihre Verknüpfung dar.

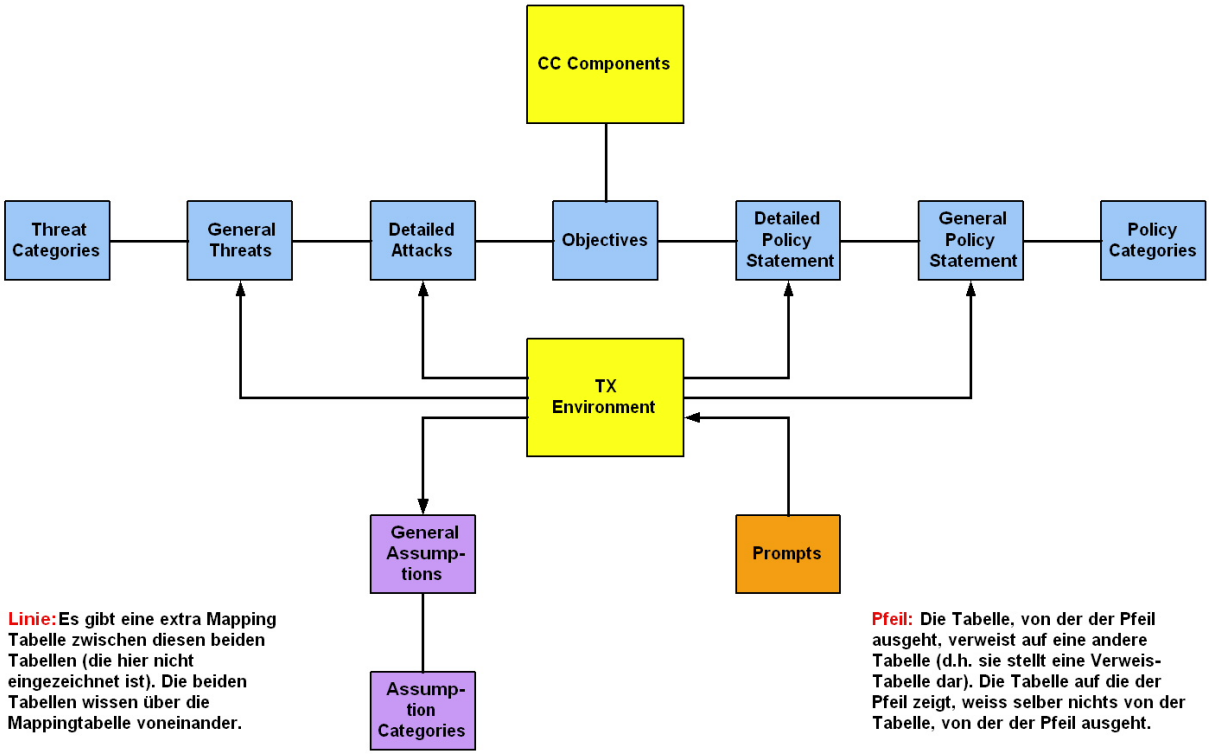

CC Components
Threat Categories
General Threats
Detailed Attacks
Objectives
Detailed Policy Statement
General Policy Statement
Policy Categories
TX Environment
General Assump-tions
Prompts
Assump-tion Categories
Linie: Es gibt eine extra Mapping Tabelle zwischen diesen beiden Tabellen (die hier nicht eingezeichnet ist). Die beiden Tabellen wissen über die Mappingtabelle voneinander.
Pfeil: Die Tabelle, von der der Pfeil ausgeht, verweist auf eine andere Tabelle (d.h. sie stellt eine Verweis-Tabelle dar). Die Tabelle auf die der Pfeil zeigt, weiss selber nichts von der Tabelle, von der der Pfeil ausgeht.

Abbildung 18

Wie aus der Grafik zu entnehmen, ist in der CCPKB die zu definierende Umgebung der Dreh- und Angelpunkt. Von ihr aus sind Bedrohungen, Angriffe, Sicherheitsziele und Annahmen über die Umgebung verknüpft. In der Prompt-Tabelle befinden sich Fragen an den Benutzer der CC Toolbox, die in der CC Toolbox dann in einem Interview beantwortet werden können. Von der zu definierenden Umgebung gelangt man indirekt zu den Sicherheitszielen, die mit den CC Komponenten verknüpft sind. Auf Basis der ausgewählten CC Komponenten werden dann in der CC Toolbox die PPs und STs erstellt.

Damit der Benutzer der CCPKB nicht direkt in den Tabellen seine Umgebung definieren muss, wird in Access ein Tool angeboten, das mittels Formularen Benutzereingaben in die CCPKB speichert und dabei auf ihre Zulässigkeit überprüft. Die Oberfläche des Tools wird in der nachfolgenden Grafik dargestellt. Für eine Erläuterung der Funktionalität dieses Tools wird auf das Handbuch der CCPKB verwiesen.

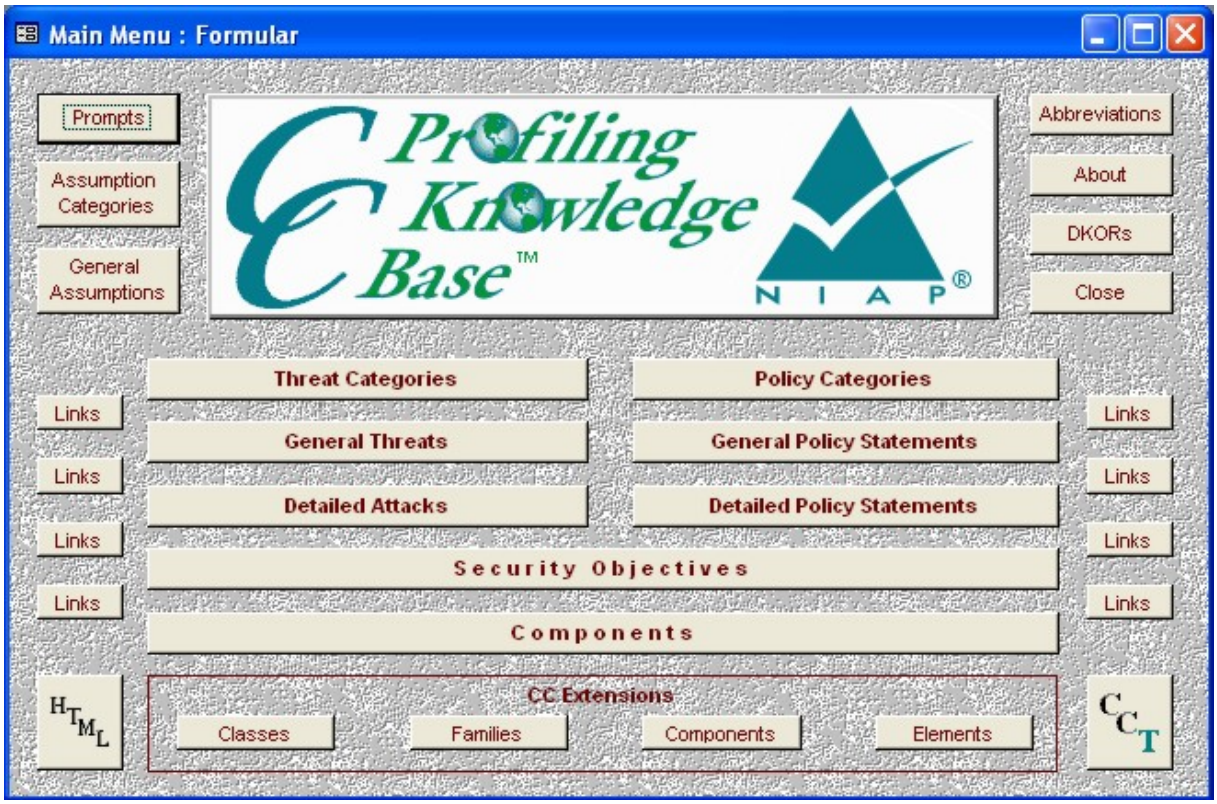


Abbildung 19

Wenn der Benutzer seine Einstellungen in der CCPKB abgeschlossen hat, kann er einen Export seiner Daten vornehmen, um sie der CC Toolbox bekannt zu machen. Neben der schon vordefinierten Umgebung des US-Verteidigungsministeriums (DKV5-0-0) kann dann auch die selbst definierte Umgebung beim Start der CC Toolbox ausgewählt werden.

Abbildung 20

Die CCPKB muss nicht genutzt werden, wenn man nur die Einstellung des US-Verteidigungsministeriums nutzen will, sie kann aber bei einer individuelleren Handhabung der CC Toolbox auf jeden Fall sinnvoll sein.

5.2 Die CC Toolbox

Die sechste Version der CC Toolbox ist die aktuellste Version und stammt aus dem Jahre 2001. Seitdem wurde die CC Toolbox nicht mehr weiterentwickelt und ist im Laufe der letzten Jahre aus ihrem offiziellen Downloadarchiv des NIST verschwunden. Dieser Vorgang ist unverständlich, da von Common Criteria seitdem keine neue Version mehr veröffentlicht wurde und die CC Toolbox daher immer noch dem aktuellen Standard entspricht. Und selbst wenn 2005 die neue CC Version 3.0 erscheinen wird, so wäre die CC Toolbox mit dem beiliegenden Sourcecode immer noch für einen Java-Programmierer auf den neuen Stand zu bringen.

Obwohl sich CC Version 2.1 bis Anfang 2005 noch nicht verändert hat, gab es doch seit 2001 einige Systemumgebungsänderungen, an die die CC Toolbox noch nicht angepasst ist. Die CC Toolbox ist vollständig in Java implementiert und daher plattformunabhängig einsetzbar, allerdings wurden bei der Implementierung Java Funktionen der Java Runtime Environment 1.3 verwendet, die ab der Version 1.4 auf den Status „deprecated" gesetzt wurden und daher nicht mehr gültig sind. Es empfiehlt sich daher die ältere Java Version 1.3 zu installieren.

Es soll im Folgenden keine ausführliche Beschreibung erfolgen, wie die CC Toolbox benutzt wird, da die beiliegenden Handbücher völlig ausreichend und verständlich sind. Dennoch sollte hier für das Verständnis auf einige Details eingegangen werden.

Nach der Installation der CC Toolbox kann die Toolbox gestartet werden. Ein Dialog fragt den User, welche vordefinierten Umgebungsannahmen er verwenden möchte (Abbildung 20). Diese Umgebungsannahmen sind aus der CCPKB generiert und exportiert worden und stehen daher der Toolbox zur Verfügung. Sie beschreiben die Zusammenhänge zwischen Annahmen, Bedrohungen, Sicherheitspolitiken, Sicherheitszielen und den Komponenten der CC. In der CCPKB liegen diese Informationen in Tabellenform vor und können dort verändert werden. Außerdem können Fragen definiert werden, die in einem so genannten Interview in der Toolbox gestellt werden. Abbildung 21 zeigt die CC Toolbox nach ihrem Start.

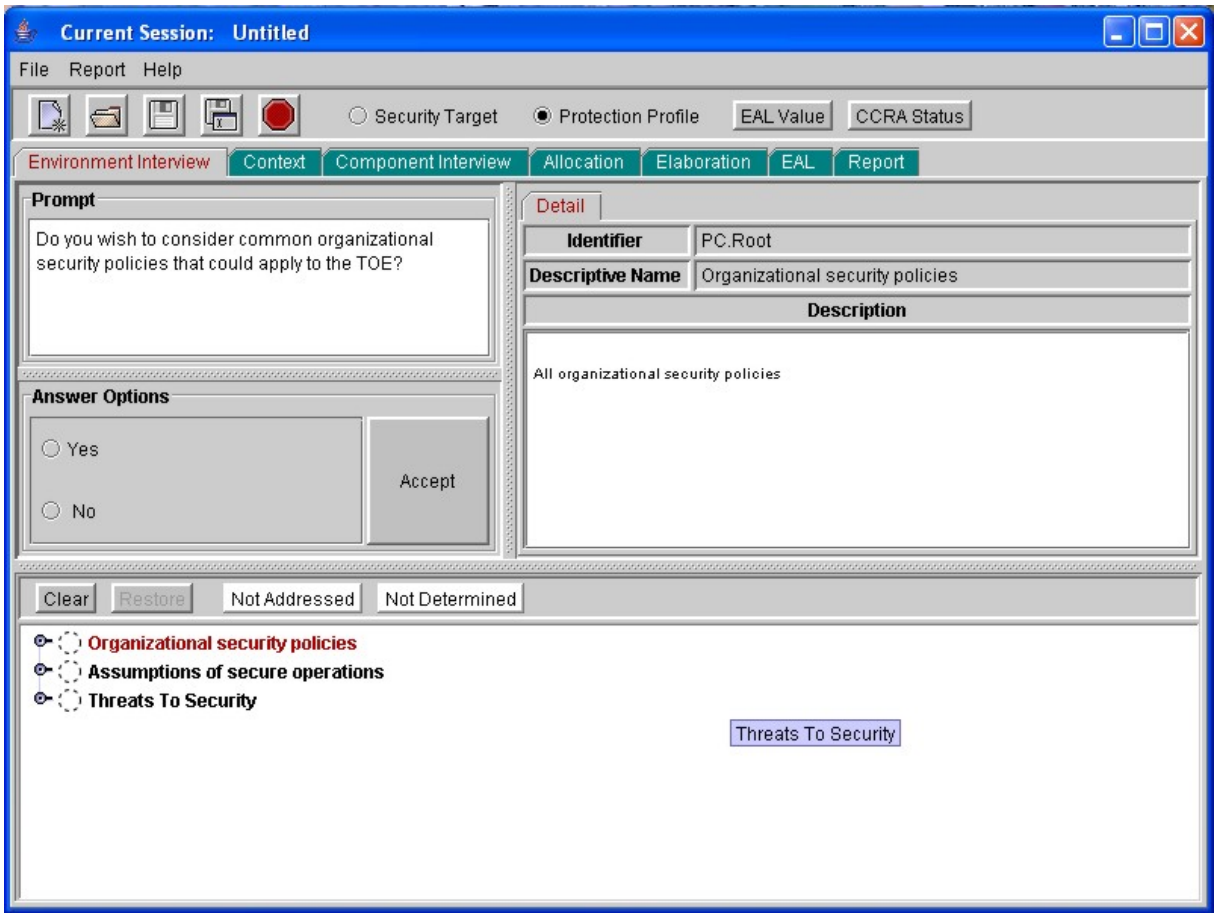


Abbildung 21

Im Kasten „Prompt“ werden dem Benutzer die Interviewfragen gestellt. Er kann sie nun beantworten, um damit später Sicherheitsziele zu definieren, die dann durch ihnen zugeordnete CC Komponenten realisiert werden. Betrachten Sie an dieser Stelle Abbildung 18, falls Ihnen der Zusammenhang noch unklar erscheint.

Die Toolbox kann anhand der Tabs von links nach rechts durchgegangen werden. Mit den jeweils getroffenen Einstellungen und Antworten auf die Interviews werden im Hintergrund Verknüpfungen anhand der Definitionen in der CCPKB bzw. der vordefinierten Umgebung gemacht. Das Ziel dieser Verknüpfungen ist, für jede Bedrohung eine entsprechende CC Komponente bereit zu stellen, um die Bedrohung zu bekämpfen. Im Tab „Report“ kann dann ein PP oder ST angeschaut werden, in dem die ausgewählten CC Komponenten automatisch aufgeführt werden. Im Menüpunkt „Report“ kann dieser dann exportiert und gedruckt werden. Der Tab „EAL“ (siehe Abbildung 22) zeigt an, ob die ausgewählten Vertrauenswürdigkeitskomponenten einer EAL entsprechen, bzw. welcher EAL sie entsprechen. Dabei wird auch angezeigt, ob eine Komponente vielleicht sogar über eine EAL-Stufe hinausgeht.

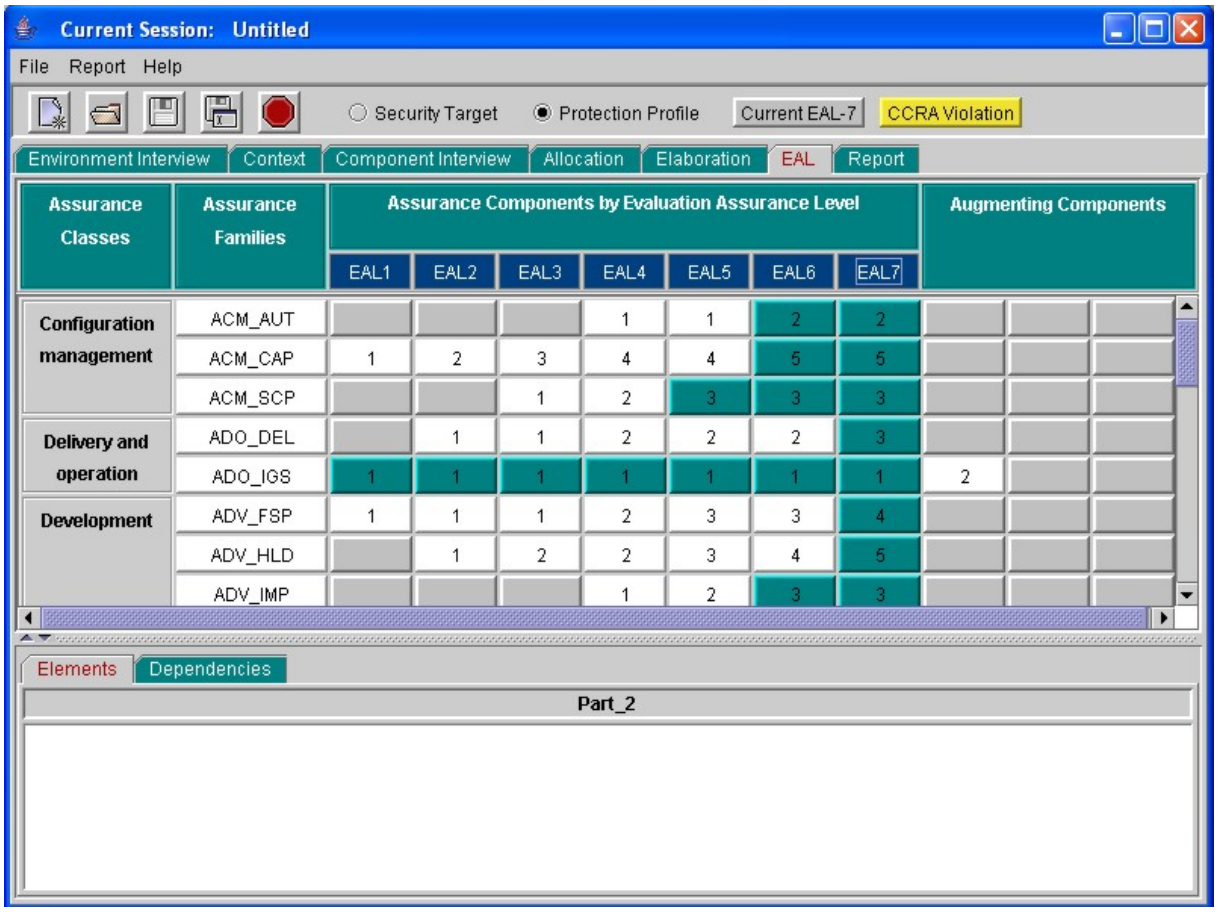


Abbildung 22

Der in Abbildung 22 gelbe Hinweis „CCRA Violation“ tritt auf, wenn eine höhere EAL Stufe, als die Stufe 4 für mindestens eine Vertrauenswürdigkeitsfamilie gewählt wird. Das hat folgenden Hintergrund: „Im Mai 2000 wurde zwischen verschiedenen nationalen Zertifizierungsstellen ein Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC geschlossen. Dieses Abkommen (CCRA) betrifft Zertifikate für Schutzprofile und Produkte bis zu einer Prüftiefe EAL 4.“ [24)] Das heißt, höhere EAL Stufen werden unter Umständen nicht in jedem Land oder von jeder Firma akzeptiert.

5.3 Das Radio Commander PP

Das Ergebnis des Einsatzes der CC Toolbox ist ein selbst erstelltes standardisiertes Protection Profile für den zukünftigen Siemens internen Gebrauch. Es soll allgemeingültig sein für eine Vielzahl von Siemens Systemen und nur noch jeweils angepasst werden müssen. Das evaluierte IT-Produkt heißt Radio Commander und unterstützt die Steuerung von Mobilfunkantennen. Mit dem PP und dieser Diplomarbeit soll die Einführung von CC bei Siemens unterstützt werden.

Das erstellte Schutzprofil "Radio Commander PP" zur Anwendung im Rahmen der Common Criteria wurde mit der Zielsetzung erstellt, grundlegende Sicherheitsanforderungen für die Entwicklung, den Betrieb und die Beschaffung aller IT-Systeme einer Radio Commander Infrastruktur, zu definieren.

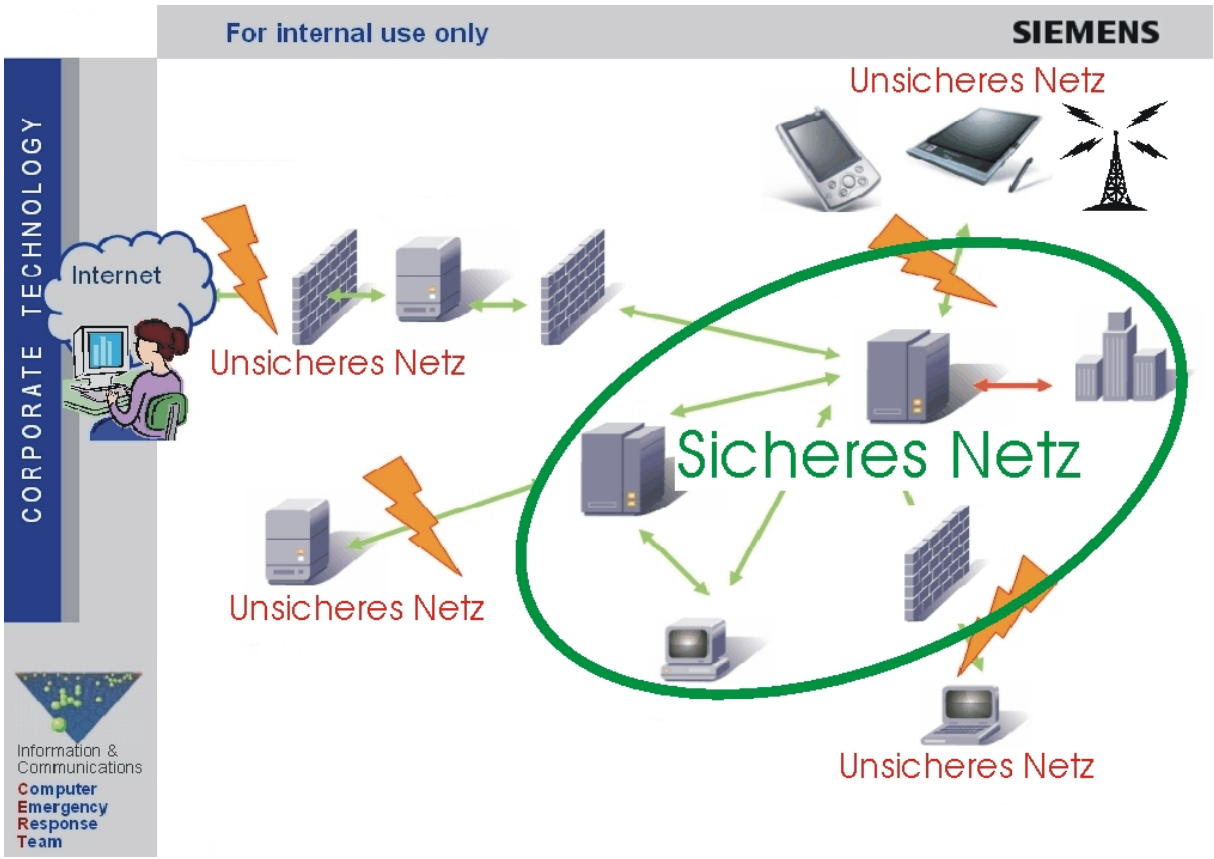


Abbildung 23

Das vorliegende Schutzprofil definiert einen Satz grundlegender Sicherheitsanforderungen zur Absicherung von IT-Systemen, wie sie typischerweise in einer Radio Commander Infrastruktur zum Einsatz kommen. Das Schutzprofil kennzeichnet dabei die Sicherheitsanforderungen an ein IT-Gesamtsystem, welches aus Arbeitsplatzrechnern, Servern, Hosts und den sie verbindenden Netzkomponenten und der zum Betrieb der Anwendungen notwendigen Software bestehen kann.

Dieses Schutzprofil ist daher auf Systeme anwendbar, die sich aus Hardwarekomponenten, Betriebssystemen, system- und anwendungsnaher Software (sog. Middleware) sowie Anwendungsprogrammen zusammensetzen. Die zum Betrieb eines solchen Gesamtsystems erforderliche bauliche, organisatorische und personelle

Infrastruktur muss bestimmten Sicherheitsanforderungen genügen, die nicht durch den EVG realisiert werden. Daher werden bestimmte Annahmen über die Betriebsumgebung gemacht, ohne die die Sicherheit des IT-Gesamtsystems nicht gewährleistet werden kann. Diese Annahmen finden sich in Abschnitt 4.1.1. des PP wieder. Die Verfügbarkeit der Informationen muss weitestgehend gewährleistet sein, insbesondere sind keine unbemerkten und nicht wieder herstellbaren Verluste von geschäfts- und sicherheitsrelevanten Daten tolerierbar.

Systeme, die dem Radio Commander Schutzprofil genügen, sind in der Lage, Zugriffe auf die von ihnen verwalteten Informationen zu kontrollieren, bei der sowohl Zugriffe einzelner Benutzer und Benutzergruppen auf Objekte, die die Informationen enthalten, auf der Grundlage der Ihnen erteilten Zugriffsrechte, als auch Zugriffe einzelner Benutzer auf anwendungskontrollierte Objekte und Funktionen auf der Basis der von Ihnen ausgeübten Rollen möglich sind.

Das Radio Commander Schutzprofil bietet einen Schutz, der für eine Umgebung angemessen ist, in der der Zugriff auf Informationen und Systemressourcen auf dazu berechtigte Benutzer beschränkt werden muss. Dabei sind die Benutzer im Rahmen der Ihnen zugeteilten Rechte als vertrauenswürdig anzusehen. Dies gilt insbesondere auch für den Umgang der Benutzer mit den Informationen, deren Dateneigentümer sie sind. Es ist jedoch erforderlich, sie für jede ihrer Aktionen jederzeit zur Verantwortung ziehen zu können. Siemens CERT fordert mit dem Radio Commander Protection Profile daher eine Reihe von Schutzmechanismen. Zu diesen Schutzmechanismen gehören neben der oben spezifizierten Zugriffskontrolle die Möglichkeit einer starken Authentisierung sowie die Möglichkeit einer umfassenden Protokollierung und Beweissicherung. Von anderen Schutzprofilen unterscheidet sich Radio Commander dadurch, dass es Sicherheitsanforderungen für die Betrachtung von Gesamtsystemen und nicht für einzelne Komponenten formuliert; neben einer rollenbasierten Zugriffskontrolle eine benutzerbestimmte Zugriffskontrolle unter der Voraussetzung vertrauenswürdige Dateneigentümer toleriert; Anforderungen und Ergebnisse bezüglich der IT-Sicherheit berücksichtigt, die von den Erfahrung bisheriger Evaluierungen von IT-Systemen im Rahmen von Siemens basieren.

Das vorliegende Radio Commander PP genügt der Vertrauenswürdigkeitsstufe EAL-4. Folgenden in Abbildung 24 markierten Vertrauenswürdigkeitsklassen wird dabei genüge getan:

Assurance Classes	Assurance Families	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4
Maintenance of assurance	AMA_AMP							
	AMA_CAT							
	AMA_EVD							
	AMA_SIA							

Abbildung 24

Das vollständige Radio Commander PP liegt im Anhang bei und stellt den praktischen Teil dieser Diplomarbeit dar. Weitergehende Erklärungen zum Radio Commander PP befinden sich im PP selbst.

5.4 Fazit der CC Toolbox

Auf den ersten Blick erscheint die genannte Erstellungszeit eines PP sehr groß, allerdings wäre die Anfertigung eines PP per Hand und ohne Toolunterstützung um ein Vielfaches größer. Denn durch die vordefinierten Verknüpfungen, die in der CCPKB gemacht wurden, wird viel Arbeit für den Ersteller eines PP abgenommen. Trotz alledem muss der Ersteller des PP jede Frage sorgfältig beantworten und den Evaluationsgegenstand genau kennen, um ein exaktes PP erstellen zu können. Dies kostet viel Zeit, aber ohne das Tool würde es noch mehr Zeit in Anspruch nehmen, so lautet die Erkenntnis von Herrn Ingruber nach Fertigstellung des Beispiel PP für den Radio Commander.

Die CC Toolbox bietet genauso wie die CCPKB gute Handbücher und Tutorials und ist daher für jemanden, der mit Evaluierungen vertraut ist, leicht verständlich. Hinzu kommt, dass der individuellen Weiterentwicklung des Tools eigentlich kaum Grenzen gesetzt sind, da neben der CCPKB auch der komplette Sourcecode mit ausgeliefert wird. Mit jetzt schon fast 500 bestehenden Javaklassen kann der Weiterentwicklungsaufwand allerdings auch schnell wachsen. Eine weitere Grenze der CC Toolbox ist, dass die eigentlichen CC Komponenten und ihre Abhängigkeiten nicht in der CCPKB stehen und bei einer neuen Version der CC Anpassungen direkt im Sourcecode gemacht werden müssten.

Die Zukunft der CC Toolbox hängt also unweigerlich mit der Zukunft von CC zusammen. Denn nur wenn die CC Toolbox bei einer neuen CC Version auch weiterentwickelt und angepasst wird, hat sie Chancen weiterhin Verwendung zu finden. Nach Rücksprache mit Dr. Mackenbrock vom BSI ist bisher für die Mitte des Jahres 2005 kommende CC Version 3.0 weder die Weiterentwicklung der CC Toolbox noch die eines anderen Tools geplant.

6. Die Zukunft von Common Criteria

Durch den Einsatz von CC wurden laut der Direktorin vom NIAP, Jean Schaffer, große Erfolge erzielt: „So far, 100 percent of the products evaluated have been approved, she said. The testing directly improved 30 percent of the products tested by eliminating security flaws that could have been exploited by attackers. About 40 percent of the products evaluated were improved by the addition or extension of security features, Schaffer said." [25)]

Damit diese Entwicklung auch in Zukunft so bleibt und CC noch mehr Einsatz finden wird, sind die an der Erstellung von CC beteiligten Institutionen zurzeit mit der Entwicklung der neuen Version 3.0 beschäftigt.

6.1 Die Version 3.0

Nach der 5. Internationalen Common Criteria Konferenz (ICCC) Ende September 2004 in Berlin hat Dr. Markus Mackenbrock vom BSI bekannt gegeben, dass im Jahre 2005 die neue Version 3.0 der Common Criteria veröffentlicht wird. [24)] In einem Telefoninterview im Dezember 2004 teilte er mir folgende Details über die neue Version mit:

Die neue Version wird voraussichtlich zwischen Mai und Juli 2005 veröffentlicht werden. Im Anschluss daran wird definitiv eine ISO Standardisierung für die neue Version von CC beantragt, so dass ungefähr ein Jahr später, 2006, die ISO Standardisierung Gültigkeit erlangen wird. Dr. Mackenbrock erwartet, dass aber schon während der ISO Standardisierungsphase im Herbst 2005 die ersten Anträge auf eine Zertifizierung nach der neuen CC Version beim BSI eingereicht werden. Die Wirtschaft wird nicht erst auf eine ISO Veröffentlichung warten, da sich im Normalfall nichts mehr an der Version ändern wird, so ist sich Dr. Mackenbrock sicher.

Das Hauptaugenmerk bei der Überarbeitung der jetzigen CC Version liegt auf der Einbindung von praktischen Erkenntnissen. Die Zertifizierung soll einfacher werden, daher sollen bisher redundante Anforderungen herausgenommen werden. Weiterhin sollen kleine Fehler behoben werden. Dr. Mackenbrock verspricht aber, dass sich an den EAL-Stufen nichts ändern wird, ebenso wie am Zertifizierungsprozess an sich. Dennoch bezeichnet er die Änderungen als „mittel tief greifend", da die Struktur der Sicherheitsziele vollständig erneuert und der 2. Teil der CC auch komplett überarbeitet werden wird.

In Anbetracht der obigen Vorstellung der CC Toolbox als Hilfsmittel zur Erstellung von PPs und STs habe ich Dr. Mackenbrock gefragt, ob das Programm auch weiterhin für CC einsetzbar sein wird. Leider sei keine Weiterentwicklung mit dem NIST oder Sparta geplant, daher wird die CC Toolbox aufgrund der Änderungen nicht mehr verwendbar sein. Es seien auch keine anderen unterstützenden Tools geplant, solange nicht die neue Version fertig gestellt sei. Wann man also überhaupt mit einem neuen Tool oder einer überarbeiteten CC Toolbox rechnen kann sei ungewiss und wohl frühestens nach der erstmaligen Veröffentlichung der Version 3.0 realistisch.

6.2 Ziele und Chancen für CC

Die Unabhängigen Zertifizierungen werden bei den Bemühungen um mehr Sicherheit in der IT immer wichtiger. Sie bilden eine notwendige Ergänzung zu herstellerspezifischen Anstrengungen wie Microsofts Next Generation Secure Computing Base (NGSCB), sind international anerkannt, öffentlich zugänglich und werden von unabhängigen Zertifizierungsstellen vergeben. [24)]

„Eigenständige und offen zugängliche Kriterien und Standards haben den Vorteil, dass sie das Vertrauen der Anwender in die IT-Sicherheit erhöhen können. Allgemein anerkannte Maßstäbe versetzen Unternehmen in die Lage, auch zu überprüfen, was Sicherheitssysteme tatsächlich tun. Die dadurch erzeugte Transparenz fördert das Vertrauen und die Verlässlichkeit in neueste Technologien." [4)]

Da die CC Version 2.1 auf allen anderen wichtigen Standards aufsetzt, wie in Abbildung 2 zu erkennen ist, stellt CC die Spitze der Hierarchie aller wichtigen IT-Standards dar. Die Version 2.1 soll aber noch nicht das Ende der Entwicklung von CC sein, denn „Zur Fortentwicklung der CC wurde von den auf Basis der CC zertifizierenden nationalen Stellen die CCIMB-Arbeitsgruppe gegründet (Common Criteria Interpretations Management Board), die in Zusammenarbeit mit der ISO die CC überarbeitet. Grundlage dieser Überarbeitungen ist eine Vielzahl von Interpretationsanfragen von Anwendern der CC, insbesondere von Prüfstellen. Diese Anfragen und Anregungen resultieren weitestgehend aus den bei Zertifizierungsverfahren gewonnenen Erfahrungen. War es das Ziel der CC Version 2.1 eine hohe Flexibilität bei der Kriterienanwendung sowie eine Kompatibilität zu den Vorläuferkriterien (TCSEC, ITSEC, CTCPEC) zu garantieren, so zielt die jetzige Überarbeitung einerseits auf eine eindeutige und optimale Anwendung der CC hin, andererseits werden aber auch verstärkt wirtschaftliche Aspekte berücksichtigt wie zum Beispiel der Verzicht auf redundante Anforderungen. Schließlich haben sich in den letzten Jahren auch die Anwendungsgebiete (Produkttypen) der CC-Zertifizierungen geändert." [24)]

Die CCIMB-Arbeitsgruppe und die ISO arbeiten laut dem BSI zurzeit also intensiv an der Weiterentwicklung der Common Criteria. Die Veröffentlichung der neuen Version 3.0 ist Mitte 2005 geplant. „Ziel dieser Überarbeitung ist es, die Attraktivität und Wirtschaftlichkeit von CC-Zertifizierungen zu erhöhen." [24)]

Es ist kein Ende des Erfolgs von CC in Sicht. Im Gegenteil, die Bemühungen eine neue CC Version zu veröffentlichen, lassen darauf schließen, dass das Interesse an CC noch weiter wächst. „The Common Criteria evaluation program continues to grow with 126 products in evaluation as of September 2004 compared with about 60 products at this time last year. We're taking in six new products or more per month" [25)] teilt Jean Schaffer stellvertretend für die USA mit.

Allerdings scheuen trotzdem noch viele Hersteller eine CC-Zertifizierung, da „Aufwand und Kosten mit der Prüftiefe steigen … Aus diesem Grund will das BSI die selektive Tiefenprüfung sicherheitsspezifischer Komponenten mit einer flächendeckenden Verbreitung von Sicherheitsprüfungen (wenn auch auf niedrigem Niveau) ergänzen. Die Schwelle zum Einstieg in CC-Evaluierungen muss also erniedrigt werden, das heißt das

deutsche Interesse besteht darin, EAL1-Evaluierungen zu erleichtern und zu fördern." [24] Diese Maßnahmen des BSI zeigen den politischen Willen nicht nur Deutschlands, sondern aller an der CC Erstellung beteiligten Staaten, CC als Standard der Zukunft zu etablieren.

Es ist aber auch zu erwarten, dass CC nicht nur von der Politik gefördert, sondern auch von der Wirtschaft angenommen wird, da ein großes Interesse vorhanden zu sein scheint. „Bei der nationalen und internationalen Normierung wird aus der Industrie immer wieder gefordert, dass sich das BSI als Dienstleister für die heimische Wirtschaft versteht und in den Normungsgremien entsprechend aktiv mitarbeitet." [24]

Diese Kombination aus politischem und wirtschaftlichem Interesse an der international anerkannten Zertifizierung nach Common Criteria machen die Tendenz deutlich: CC wird sich als Standard der Zukunft durchsetzen.

Abbildungsverzeichnis

1) Abbildung aus BSI-Sicherheitszertifikate; http://www.bsi.de/literat/faltbl/sichzerb .htm; Bundesamt für Sicherheit in der Informationstechnik

2) Abbildung aus Datenschutz und Datensicherheit; http://www.uni-koblenz.de/~ moeh/lehre/ws0304/; Michael Möhring Vorlesungsskript Universität Koblenz/ Lindau

3) Abbildung aus Die TCSEC Kriterien(Orange Book); http://www.kecos.de/script/ 31obook.htm; Prof. Dr. Hans Jürgen Ott

4) Abbildung aus Common Criteria (ISO/IEC 15408); Faltblatt F06CC; Bundesamt für Sicherheit in der Informationstechnik

5) Abbildung aus IT Sicherheit auf Basis der Common Criteria – ein Leitfaden; Bundesamt für Sicherheit in der Informationstechnik

6-17) Abbildungen aus Common Criteria Version 2.1; Bundesamt für Sicherheit in der Informationstechnik

18) Eigenes Diagramm

19) Eigener Screenshot der CC Profiling Knowledge Base

20-22) Eigene Screenshots der CC Toolbox

23) Abbildung von Siemens CERT

24) Eigener Screenshot der CC Toolbox

Tabellenverzeichnis

1) Tabelle aus TCSEC und ITSEC; http://www.tecchannel.de/betriebssysteme/ 1282/0.html; tecCHANNEL

2) Eigene Tabelle; aufbauend auf: Common Criteria Version 2.1; Bundesamt für Sicherheit in der Informationstechnik

3) Tabelle aus TCSEC und ITSEC; http://www.tecchannel.de/betriebssysteme/ 1282/0.html; tecCHANNEL; erweitert um die EAL-Stufe 0

Literaturverzeichnis

Online Artikel und Online Ressourcen

Alle Online Artikel und Online Ressourcen liegen auf CD bei.

1) Common Criteria (ISO/IEC 15408); Faltblatt F06CC; Bundesamt für Sicherheit in der Informationstechnik

2) IT-Sicherheitskriterien; http://www.bsi.de/zertifiz/itkrit/itkrit.htm; Bundesamt für Sicherheit in der Informationstechnik

3) IT-Security-Evaluation; http://www.gi-ev.de/praxis/hit/cc-itsec.html; Hitforum - Ein Praxisforum der Gesellschaft für Informatik e.V.

4) TCSEC und ITSEC; http://www.tecchannel.de/betriebssysteme/1282/0.html; tecCHANNEL

5) CTCPEC; http://www.it-administrator.de/lexikon/ctcpec.html; IT Administrator

6) CTCPEC; http://www.demonium.de/th/home/sicherheit/lexikon/buchstabe_c.phtml; Lexikon der Informationssicherheit

7) Datenschutz und Datensicherheit; http://www.uni-koblenz.de/~moeh/lehre/ws0304/; Michael Möhring Vorlesungsskript Universität Koblenz/Lindau

8) Schutzprofile nach Common Criteria; Faltblatt F06CC; Bundesamt für Sicherheit in der Informationstechnik

9) Common Criteria Version 2.0 fertiggestellt; Ulrich van Essen, Bundesamt für Sicherheit in der Informationstechnik

10) Einführung in die Evaluierung nach Common Criteria; Bundesamt für Sicherheit in der Informationstechnik

11) Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik; Dr. Eckart Brauer und Ulrich van Essen; Bundesamt für Sicherheit in der Informationstechnik

12) IT Sicherheit auf Basis der Common Criteria – ein Leitfaden; Bundesamt für Sicherheit in der Informationstechnik

13) Common Criteria Version 2.1; Bundesamt für Sicherheit in der Informationstechnik

14) IT – Evaluationshandbuch; ZSI - Zentralstelle für Sicherheit in der Informationstechnik im Auftrag der Bundesregierung; Bundesanzeiger

15) Katalog der IT-Sicherheitskriterien; 1989; Bundesamt für Sicherheit in der Informationstechnik

16) ITSEC; Bundesamt für Sicherheit in der Informationstechnik

17) IT-Sicherheitszertifizierung; Bundesamt für Sicherheit in der Informationstechnik

18) Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik; Dr. Mackenbrock; Bundesamt für Sicherheit in der Informationstechnik

19) Evaluation Assurance Level (EAL); Bundesamt für Sicherheit in der Informationstechnik

20) Die TCSEC Kriterien(Orange Book); http://www.kecos.de/script/31obook.htm; Prof. Dr. Hans Jürgen Ott

21) Evaluation; http://www.secunet.de/content.php?text=k_sina_glossar; Security Networks AG

22) BSI-Sicherheitszertifikate; http://www.bsi.de/literat/faltbl/sichzerb.htm; Bundesamt für Sicherheit in der Informationstechnik

23) Studie: Hackerangriffe; http://www.intern.de/97/24/02.shtml; Internet Intern

24) Common Criteria: Version 3.0 in Kürze; http://www.kes.info/archiv/heft/04-4.htm; Bundesamt für Sicherheit in der Informationstechnik - Forum

25) NIAP chief touts Common Criteria; http://www.fcw.com/fcw/articles/2004/1025/web-niap-10-27-04.asp; FCW

26) ICCC 2004 Wrap Up; http://www.corsec.com/news_oct04.php; Corsec Security

27) Conforming to a US Government Medium Robustness Protection Profile; http://www.iccconference.com/conference-agenda/abstract-view.asp?aID=123; Bundesamt für Sicherheit in der Informationstechnik

28) How much does validation cost?; http://www.corsec.com/ccc_faq.php; Corsec Security Common Criteria FAQ

29) IT-Grundschutzhandbuch; http://www.bsi.de/gshb/; Bundesamt für Sicherheit in der Informationstechnik

30) Arrangement on the Recognition of Common Criteria Certificates; http://www.cse-cst.gc.ca/en/documents/services/ccs/ccra.pdf; Communications Security Establishment

Fachbücher

31) **Kriterien für die Bewertung der Sicherheit von Systemen in der Informationstechnik (ITSEC). Vorläufige Form der harmonisierten Kriterien;** Version 1.2; Hrsg. v. d. Europäischen Union, Bundesanzeiger-Verlag Köln; 06/1991

32) **Common Criteria for Information Technology Security Evaluation (Common Criteria 2.1);** ISO/IEC 15408; 08/1999

33) **Information technology. Code of practice for information security management;** ISO/IEC 17799:2000 (BS 7799-1:2000); 2000

34) **Information security management. Specification for information security management systems;** BS 7799-2:1999, 1999.

35) **IT-Sicherheitskriterien (ITS): Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT);** 1. Fassung; Hrsg. v. d. Zentralstelle für Sicherheit in der Informationstechnik, Bundesanzeiger Verlagsgesellschaft, Köln, 1989

36) **Trusted Computer System Evaluation Criteria (TCSEC, "Orange Book");** US DoD 5200.28-STD; Department of Defense; 12/1985

37) **Canadian Trusted Computer Product Evaluation Criteria (CTCPEC);** Version 3.0; Canadian Systems Security Centre, Communications Security Establishment, Government of Canada; 01/1993

38) **NATO Trusted Computer System Evaluation Criteria;** NATO AC/35-D/1027; 1987

39) **Proposed Technical Evaluation Criteria for Trusted Computer Systems;** M79-225; Nibaldi, G. H.; MITRE Corporation; Bedford (MA); 1979

40) **Specification of a Trusted Computing Base;** M79-228; Nibaldi, G. H.; MITRE Corporation, Bedford (MA); 1979

41) **Information Technology Security Evaluation Criteria (ITSEC);** Version 1.2; Office for Official Publications of the European Communities, 06/1991

Abkürzungsverzeichnis

B

BSI	Bundesamt für Sicherheit in der Informationstechnik

C

CC	Common Criteria for Information Technology Security Evaluation / Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
CCIMB	Common Criteria Interpretations Management Board
CCPKB	CC Profiling Knowledge Base
CCRA	Arrangement on the Recognition of Common Criteria Certificates
CEM	Common Evaluation Methodology / Gemeinsame Evaluationsmethodologie
CEMEB	Common Evaluation Methodology Editorial Board
CERT	Computer Emergency Response Team
CT	Corporate Technology
CTCPEC	Canadian Trusted Computer Evaluation Criteria

D

DAC	Discretionary Access Control
DIN	Deutsche Institut für Normung

E

EAL	Evaluation Assurance Level / Vertrauenswürdigkeitsstufe
ECMA	European Computer Manufacturers Association
EVG	Evaluationsgegenstand

I

IC	Information & Communication
ICCC	Internationalen Common Criteria Konferenz
IEC	International Electrotechnical Commission
ISO	Internationale Standardisierungsorganisation
IT	Information Technology / Informationstechnik
ITS	IT-Sicherheitskriterien
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Methodology
ITSK	IT-Sicherheitskriterien
IuKDG	Informations- und Kommunikationsdienste Gesetz

M

MAC	Mandatory Access Control

N

NGSCB	Next Generation Secure Computing Base
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency

P

PP	Protection Profile / Schutzprofil

S

SF	Security Function / Sicherheitsfunktion
SFP	Security Function Policy / funktionale Sicherheitspolitik
SigG	Signaturgesetz
SigV	Signaturverordnung
SOF	Strength of Function /Stärke der Funktionen
ST	Security Target / Sicherheitsvorgaben

T

TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation / Evaluationsgegenstand
TSC	TSF Scope of Control / Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functions / EVG-Sicherheitsfunktionen
TSFI	TSF Interface / TSF-Schnittstelle
TSP	TOE Security Policy / EVG-Sicherheitspolitik

CC Toolbox Guide

This CC Toolbox Guide is only a new composed excerpt from "Touring the CC Toolbox" to have a Quick Start Manual for using the CC Toolbox. You can also use the original version to have a Starting Manual, but this one is more compressed.

Content

1 Preface
1.1 What Is the CC Toolbox?
1.2 Who Is This Guide For?

2 Introduction
2.1 The CC Toolbox Project
2.2 What the CC Toolbox Provides
2.3 Ways of Using the CC Toolbox

3 Quick Tour of the CC Toolbox
3.1 Top-Level Interface
3.2 CC Toolbox Users Guide and Reference Manual
3.3 Environment Interview Tab
3.4 Context Tab
3.5 Component Interview Tab
3.6 Allocation Tab
3.7 Elaboration Tab
3.8 EAL Tab
3.9 Report Tab

4 Getting Started

5 Frequently Asked Questions

6 Examples

1 Preface

1.1 What Is the CC Toolbox?

The Common Criteria (CC) provides a language for describing Information Technology (IT) system security requirements. The CC paradigm includes two kinds of documents for specifying security requirements, Protection Profiles (PP)s and Security Targets (ST)s. The CC Toolbox aids Protection Profile and Security Target authors in drafting PPs and STs. It provides structured interviews to aid the novice CC user in identifying pertinent CC components.

A CC component is the smallest selectable set of security requirements from the CC that may be included in a PP or ST. In addition, it assists all users in managing the complexity inherent in such documents. The output of the CC Toolbox is a skeleton report that can be polished into a PP or ST.

1.2 Who Is This Guide For?

This document is intended for new CC Toolbox users. However, you should have a basic understanding of the CC, or be in the process of learning about the CC. In addition, you should be comfortable with using the Windows operating systems.

The CC Toolbox Guide is a supplement to and not a replacement for the Users Guide and Reference Manual provided with the CC Toolbox.

2 Introduction

2.1 The CC Toolbox Project

The CC is a language you can use to describe IT product and system security requirements or specifications. It includes both security functional and assurance components. In addition, the CC also defines operations that allow you to tailor these components into specific requirements that describe your particular security needs. You can use the security functional components to express the security functions you require in a product or system. You can use the security assurance components to express the requirements for assurance that those security functions perform correctly.

The CC also provides a grammar for organizing the security functional and assurance components into coherent security specification documents. A Protection Profile (PP) is an implementation-independent statement specifying the security requirements for a product, category of products, or systems that meet specific consumer needs. A Security Target (ST) defines the implementation-dependent security requirements and specifications to be used as the basis for the evaluation of a product or system.

Moreover, evaluations of products against the CC are covered by a Common Criteria Recognition Arrangement (CCRA). Initially this agreement was know as MRA, the Mutual Recognition Arrangement. Under the CCRA, each participating member nation agrees to recognize that evaluations carried out in the other member nations' accredited laboratories conform to acceptable technical standards. That is, if an IT product or system is evaluated by an accredited laboratory in one member nation, then the evaluation results will be accepted by all the nations participating.

The transition to the CC can be daunting despite the rewards of the common language and international recognition of evaluations. The CC provides extensive flexibility in selecting components to satisfy security objectives. Yet to ensure that the specifications are meaningful, the CC also constrains how the components can be combined in PPs and STs. The CC mandates that PPs and STs:

- Include a description of the Target of Evaluation (TOE), the IT product or system that is the subject of an evaluation;
- Describe the TOE security environment (i.e. assumptions, policies, and threats) to establish the context in which the TOE is intended to be used;
- Include security objectives to address all the security environment aspects identified; and
- Tailor the security functional and assurance components to meet the security objectives.

Finally, the PP and ST authors must provide rationale to link together the TOE description, the security environment, the security objectives, and the security functional and assurance requirements into a coherent whole. NIAP identified a need to help consumers and developers make the transition to the CC. One of its initiatives was to sponsor the development of software tools to help CC users take advantage of the CC's flexibility while managing its complexity. One tool was developed to help PP authors and another to help ST authors. The CC Toolbox is a common interface for these two tools and provides a common data representation. The CC Profiling Knowledge Base, a database of sample security engineering information, accompanies the CC Toolbox. The Knowledge Base can be used to update the security engineering information used in the Toolbox or as a standalone tool.

2.2 What the CC Toolbox Provides

The CC Toolbox provides you with tools for writing a PP or ST and security engineering information that support those tools. The CC Toolbox helps you do the following:

- Describe the assumptions, policies, and threats that make up the TOE security environment.
- Capture security objectives to counter threats and satisfy policies and assumptions for the TOE and its environment.
- Identify relevant CC components to satisfy an objective and incorporate them into your PP or ST.
- Apply CC operations (i.e., assignment, iteration, refinement, and selection) to tailor CC components into requirements.
- Select an Evaluation Assurance Level (EAL).
- Manage mappings that relate the TOE security environment to the security objectives and relate security objectives to requirements.
- Build rationale arguments required by the CC.
- Manage details of identification, CC component dependencies, application notes, and implementation notes.

While the CC Toolbox provides tools to help you write a PP or ST, its output is not a complete PP or ST. Rather the output of the CC Toolbox is a draft report, either a PP or ST. You as the author must flesh out this draft with complete rationale as specified by the CC. Generally, you will also need to format the draft version of a PP or ST to meet your specific style requirements.

2.3 Ways of Using the CC Toolbox

The tasks involved in writing PPs and STs overlap significantly. You can use the CC Toolbox to write either a PP or a ST. The CC Toolbox presents a common user interface for both authoring tools.

Authors approach PP writing in different ways. Some take a top down approach and generally follow the order of the PP content presented in the CC. These authors begin with an approximate TOE description, describe the TOE security environment, write security objectives, and select and complete CC components. Other authors use a bottom up approach. They start with a given set of requirements and identify the CC components corresponding to those requirements. From the requirements, the authors build the necessary security objectives, TOE security environment, and TOE description.

Whether you prefer a top-down or bottom-up approach, it is unlikely that you will complete a PP in a single pass. You will likely need to revisit and refine sections because your understanding of your security needs and their presentation will change as you write. In particular, you will need to write rationale to support your choices of environment aspects, security objectives, and CC components. Writing rationale may reveal inconsistencies or omissions in your work, or may convince you to revise earlier decisions.

The CC Toolbox has a flexible user interface that supports both approaches to PP writing. The main window of the Toolbox has interface views corresponding to major sections of the PP. As examples, the **Context** interface presents the Toolbox features that let you describe the TOE security environment and security objectives, while the **Allocation** interface allows you to select CC components.

There are two CC Toolbox interface views that do not correspond to PP sections: the **Environment Interview** interface and the **Component Interview** interface. The **Environment Interview** interface provides structured access to the security engineering information incorporated from the CC Profiling Knowledge Base. You can mark the organizational security policies, assumptions, and threats from the Knowledge Base that are relevant to your TOE by completing an interactive interview. The CC Toolbox uses these markings to focus the information presented in the **Context** interface and to suggest related potential environmental considerations. Analogously, the **Component Interview** interface provides structured access to the CC components. The **Component Interview** helps you identify the CC components you need to meet your security objectives. Both interviews are designed to minimize asking you questions by tailoring the interview based on your answers.

The CC Toolbox interview interfaces give you another way of using the Toolbox in addition to using it as a PP editor. If you are new to the CC you can use the CC Toolbox as a translator to convert your description of your IT security needs into CC terms. You can use the **Environment Interview** and **Component Interview** interfaces to guide you efficiently to the sample security engineering information and CC components that are relevant to your IT security needs. If you are an experienced PP or ST author, you may skip the interviews.

The bottom line is that the CC Toolbox is a flexible application. With it you can browse the CC and sample security engineering information and you can edit PPs and STs. It supports a variety of authoring styles. The Toolbox has features that help both novice CC users and experienced PP and ST authors.

3 Quick Tour of the CC Toolbox

This quick tour is intended to give a high-level overview of the CC Toolbox user interface. It shows you the main interface views of the Toolbox and provides references to the *Users Guide* and *Reference Manual*. Sections 4 to 9 provide a more detailed structured description of using the CC Toolbox to write a PP. The first example here shows how to start the CC Toolbox. The second shows how to open a previously saved report data set.

Example Starting the CC Toolbox

1) Click **Start** on the Task bar and move the mouse pointer up to **Programs**.

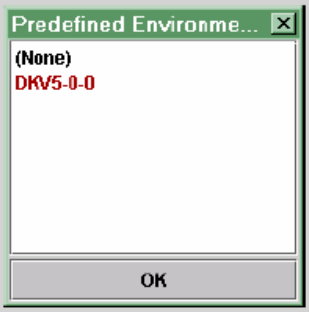
   A menu of your applications and application folders appears.

2) Move the mouse pointer over the **CC Toolbox** application folder.

   A menu of CC Toolbox applications appears.

3) Click **StartCC**.

   An MS-DOS window appears followed by the CC Toolbox start-up screen. If this is the first time you are using the CC Toolbox or you had not saved a previous report data set, the **Predefined Environment List** window appears.



4) Click **DKV5-0-0** in the **Predefined Environment List** and click the **OK** button.

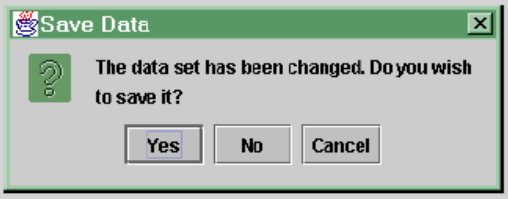
   This selects the default security engineering information from the CC Profiling Knowledge Base. If you have incorporated modified versions of the CC Profiling Knowledge Base into the CC Toolbox, there will be additional options in the list. The CC Toolbox **Top-Level** interface appears. Be patient; on a minimum configuration machine it may take two minutes for the Toolbox to start.

When the CC Toolbox starts, it resumes with the last report data set or the default **Untitled** report data set if you had not previously saved the report data set. The following example shows how to change report data sets once you have started the Toolbox.

Example Opening a Saved Report Data Set

1) Click the **File** menu, and then click the **Open** menu item from the drop down menu.

If you have changed the report data set without saving it, the **Save Data** dialog box appears.

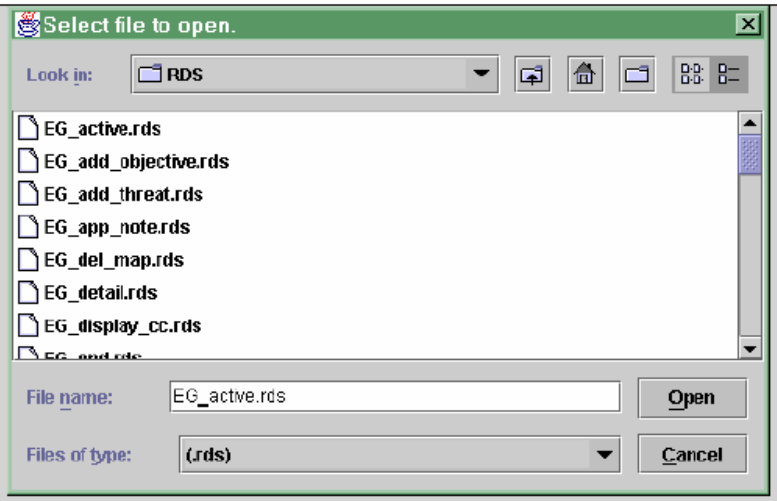


2) Click **Yes** to save your changes or **No** to discard your changes. (Clicking **Cancel** would stop the file open operation and return to the current report data set.)

A dialog box opens listing the report data sets and folders in the default folder. To display the contents of the parent folder, click the button. To display the contents of a directory in the list, double click on the directory name. The button returns you to your Windows personal folder. The button creates a new folder within the current folder. (You can configure the default directory where the CC Toolbox looks for report data set files.[19])

3) Click on the report data set you want to open, here **EG_active.rds**.

The color of your selection changes to red and the CC Toolbox copies your selection to the **File Name** text field.



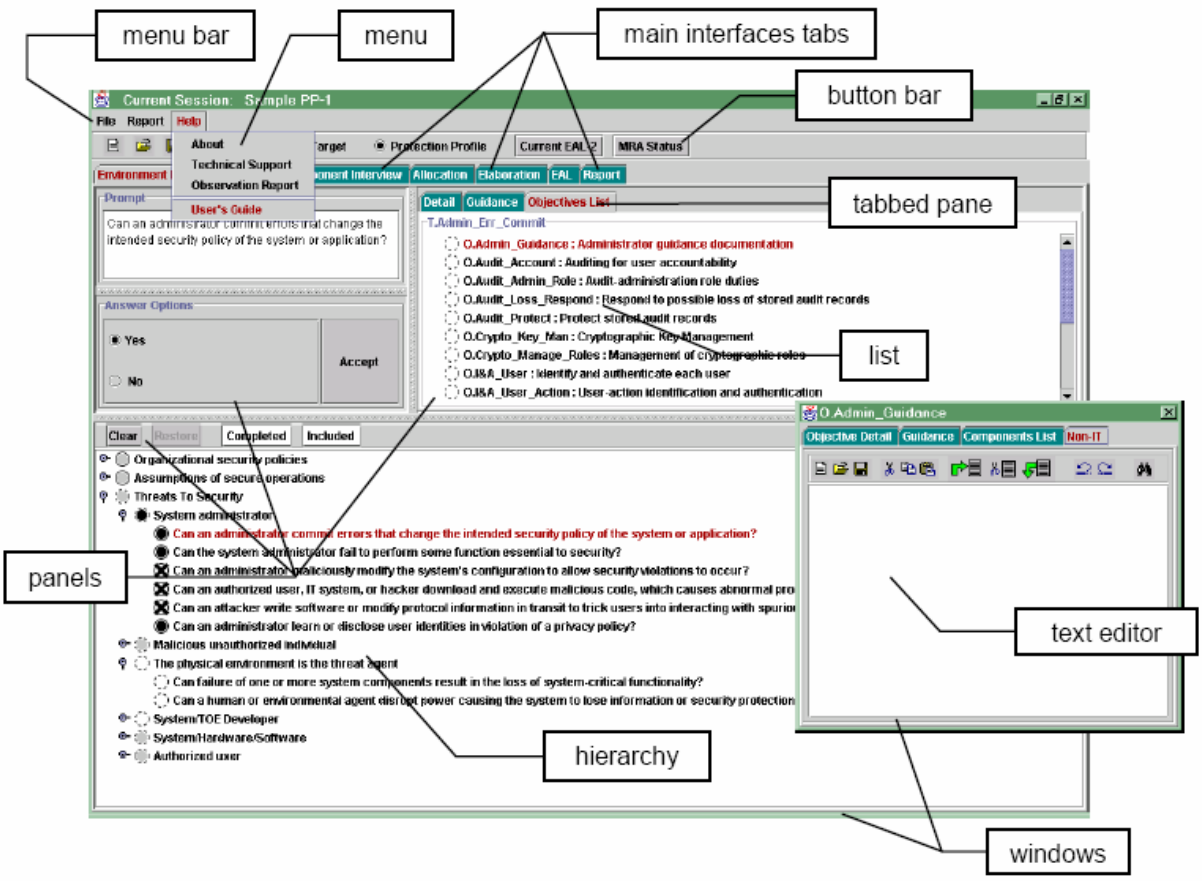
4) Click the **Open** button.

The dialog box closes and the CC Toolbox opens the report data set, e.g. **EG_active.rds**.

3.1 Top-Level Interface

You may edit one PP at a time with the CC Toolbox. To facilitate editing, the CC Toolbox user interface groups together related features into separate views called *interfaces.* You move between the main interface views using the **Top-Level** interface. The **Top-Level** interface contains a tabbed pane with one tab for each of the main interfaces. In the Toolbox, you click on an interface tab to view that interface. In addition, the **Top-Level** interface holds features shared by all the interfaces such as the title bar, the main menu bar, the toolbar, and the window controls.

Each interface contains multiple *interface components* as illustrated below. The **Environment Interview** interface, for example, contains a panel for questions and answers, a tabbed pane for additional information about the current question (here a list of security objectives related to the threat in question), and a hierarchy panel showing the structure of the interview and your responses. The *Reference Manual* provides an overview of the interface components (*Reference Manual*: Using this Document) along with more detailed descriptions (*Reference Manual*: Shared Resources: Component Types).



CC Toolbox uses a typical Windows-style main menu. The **File** menu lets you save and open report data set files. The **Report** menu lets you update the draft report to reflect changes you have made to the current report data set. You export the draft report in HTML format for polishing. The **Help** menu provides access to the *Users Guide* and *Reference Manual*. It also gives you a means of reporting problems.

Key point **Report formats**

There are three different formats used to represent your PP. The different formats are used in different contexts. These formats are:

Report Data Set (RDS)	This is the format that the CC Toolbox uses to store your information internally and on disk. Report data sets on disk have a '.rds' file extension by default.
Report	This is the format that the CC Toolbox uses for previewing and printing the PP. Toolbox processes the current report data set and formats it into a document for viewing or printing.
Exported report	This is an HTML version of the PP that can be modified by other applications, for example, a word processor. Other applications cannot work directly on RDS files. Hence the CC Toolbox can convert the internal report data set format into HTML format.

You can copy and share RDS files. However, you cannot merge RDS files.

The CC Toolbox can export a report to HTML format, but it cannot import HTML back into RDS format. So once you export the report, you can no longer edit that report with the CC Toolbox. However, the original report data set is intact. You may edit the RDS and export a new report, but any editing done to the old exported report will need to be redone to the new one.

To summarize, the formats and conversions are:

Report Data Set (internal) ⇨ Report (internal) ⇨ Exported report (external HTML)

3.2 CC Toolbox *Users Guide* and *Reference Manual*

The CC Toolbox *Users Guide* and *Reference Manual* are both available from within the Toolbox. You can keep the help documentation window and the CC Toolbox window open simultaneously and switch between them. The following example illustrates how to display the contents of the *Reference Manual*. *Reference Manual* window is an annotated copy of the same *Reference Manual* window.

Example Displaying a *Reference Manual* Section

1) Click the **Help** menu on the main menu bar.

   The menu of help item drops down.

2) Click **User's Guide** in the drop down menu.

   A new window appears containing the online documentation.

3) Click the right-hand book icon ( ).

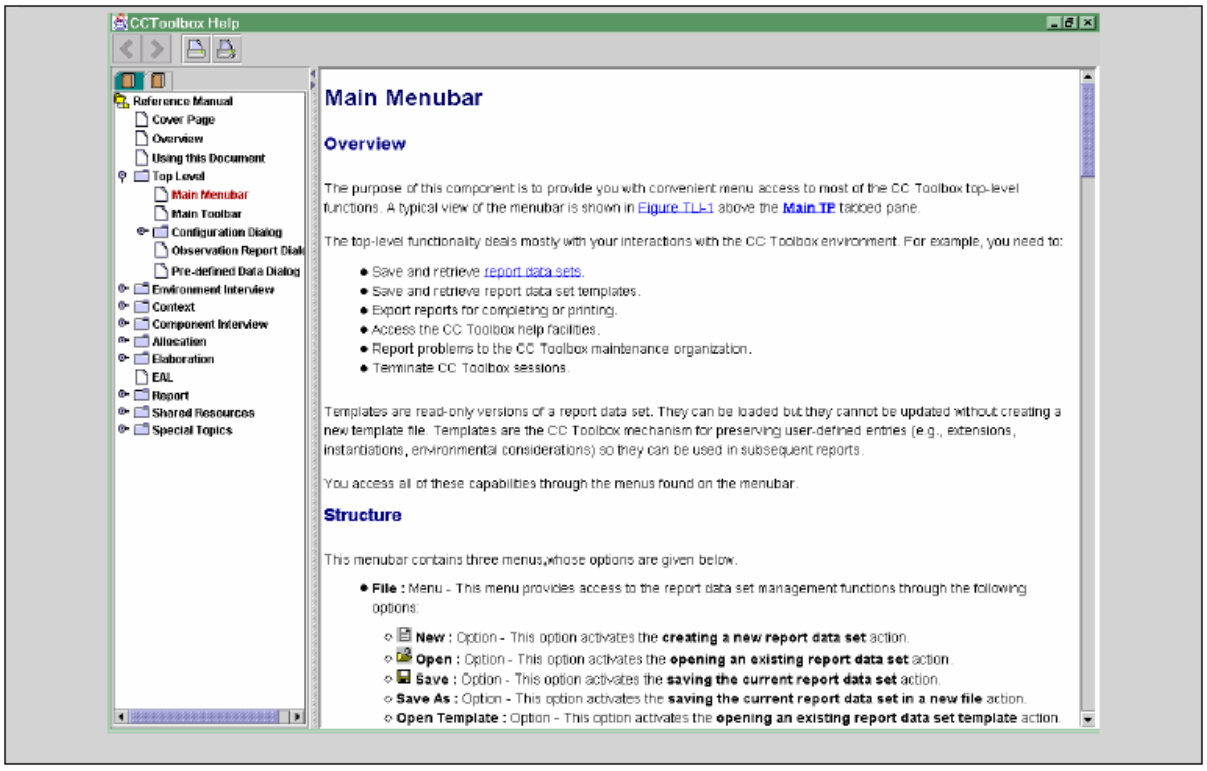
   The title of the **Table of Contents** in the left-hand panel changes from **Users Manual** to **Reference Manual**.

4) Click the expand lever ( ) to the left of **Top Level**.

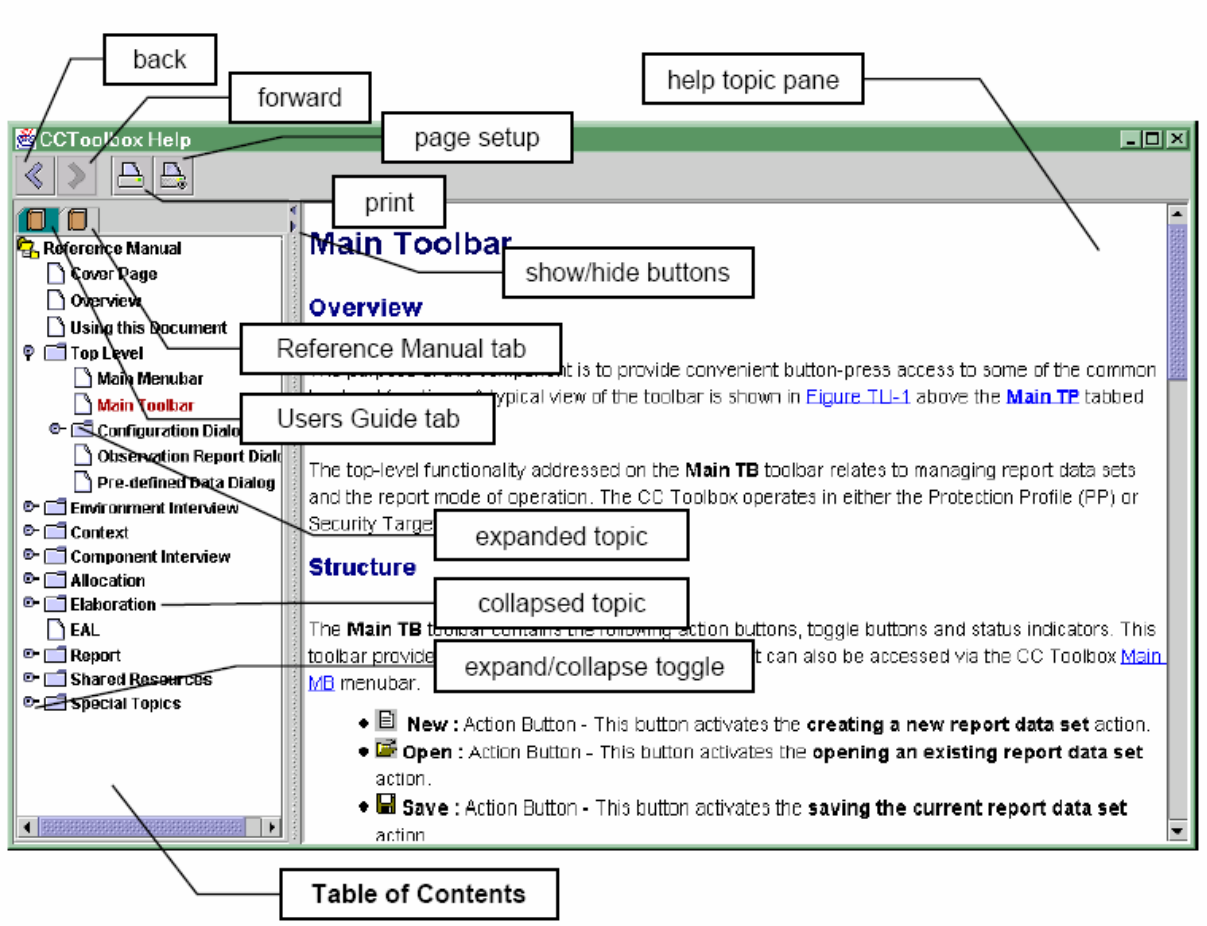
   The subsections of the **Top Level** section appear.

5) Click **Main Menubar**

   The Toolbox displays the Main Menu bar section in the right-hand panel. Your display should look similar to:


CCToolbox Help
Reference Manual
Cover Page
Overview
Using this Document
Top Level
Main Menubar
Main Toolbar
Configuration Dialog
Observation Report Dial
Pre-defined Data Dialog
Environment Interview
Context
Component Interview
Allocation
Elaboration
EAL
Report
Shared Resources
Special Topics
Main Menubar
Overview
The purpose of this component is to provide you with convenient menu access to most of the CC Toolbox top-level functions. A typical view of the menubar is shown in Figure TLL-1 above the Main TP tabbed pane.
The top-level functionality deals mostly with your interactions with the CC Toolbox environment. For example, you need to:
Save and retrieve report data sets.
Save and retrieve report data set templates.
Export reports for completing or printing.
Access the CC Toolbox help facilities.
Report problems to the CC Toolbox maintenance organization.
Terminate CC Toolbox sessions.
Templates are read-only versions of a report data set. They can be loaded but they cannot be updated without creating a new template file. Templates are the CC Toolbox mechanism for preserving user-defined entries (e.g., extensions, instantiations, environmental considerations) so they can be used in subsequent reports.
You access all of these capabilities through the menus found on the menubar.
Structure
This menubar contains three menus,whose options are given below.
File : Menu - This menu provides access to the report data set management functions through the following options:
New : Option - This option activates the creating a new report data set action.
Open : Option - This option activates the opening an existing report data set action.
Save : Option - This option activates the saving the current report data set action.
Save As : Option - This option activates the saving the current report data set in a new file action.
Open Template : Option - This option activates the opening an existing report data set template action.

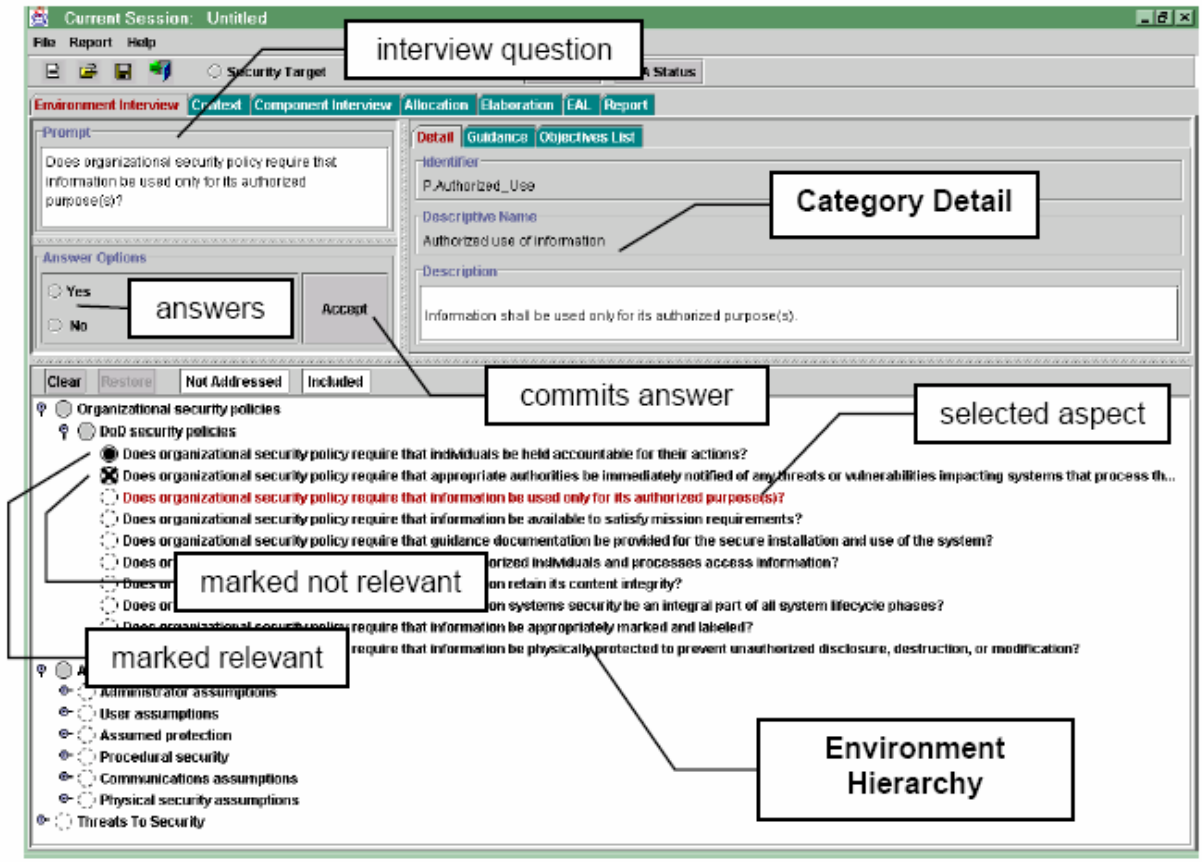
Both the *Users Guide* and *Reference Manual* are hypertext documents. Hyperlinks are underlined and shown in blue. Click on a hyperlink to move to that help topic. Click on the back button ( ) to return.



3.3 Environment Interview Tab

The **Environment Interview** interface provides structured access to the sample security engineering information incorporated from the CC Profiling Knowledge Base. The main purpose of this interface is to help you identify organizational security policies, assumptions, and threats from the Knowledge Base that are relevant in the environment of the TOE. A second purpose of the interview is to gather information that the CC Toolbox can use to suggest potentially relevant environment considerations.

The **Environment Interview** interface is made up of three interface components. The **Prompt** panel shows you the question associated with the selected environment consideration and the possible answers. The **Category Detail** tabbed pane gives you more details about the selected environmental consideration such as its descriptive name and full description. The **Environment Hierarchy** shows the structure of the interview, what environment consideration is currently selected, and the responses you have entered.

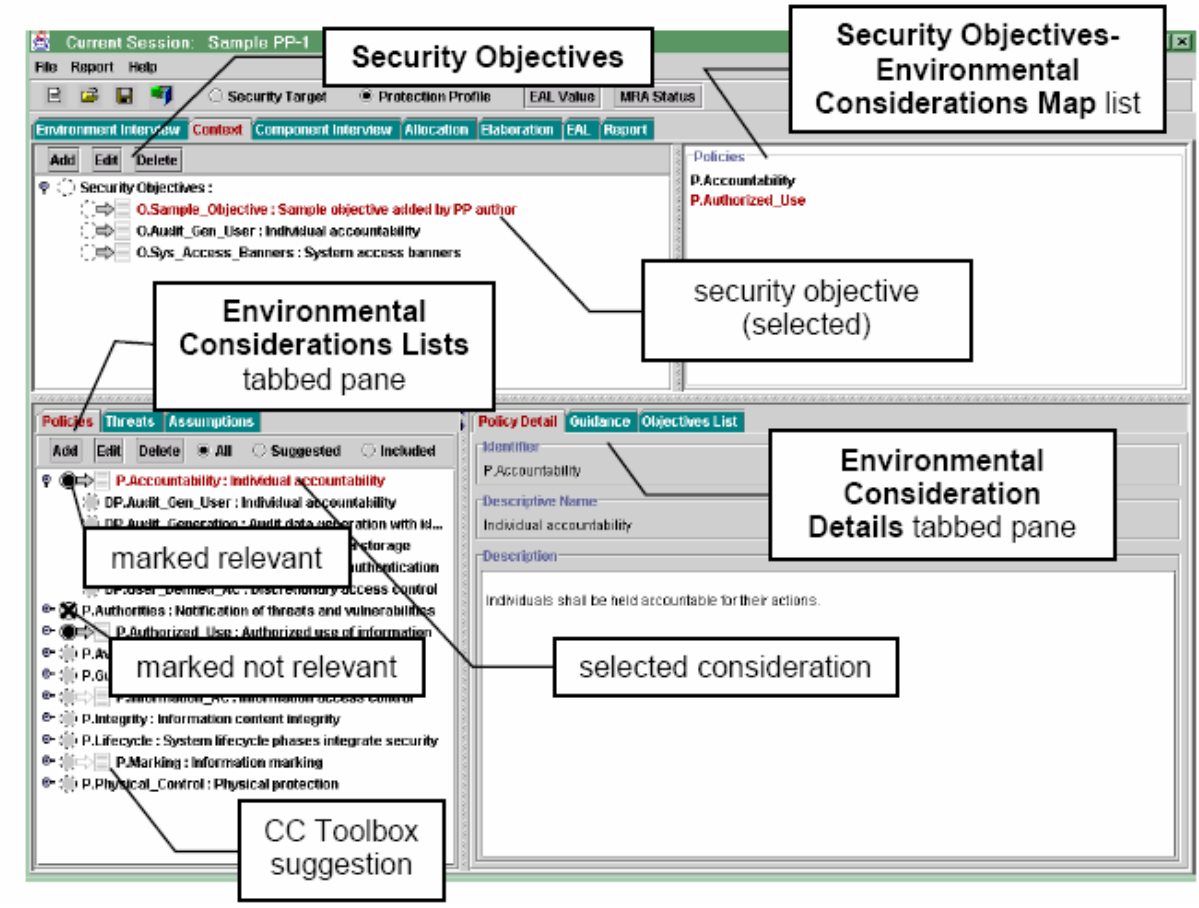


3.4 Context Tab

Context interface serves three distinct purposes. (See *Reference Manual*: Context.) You can:

- Enter TOE-specific organizational security policies, assumptions, and threats into the report data set.
- Enter TOE-specific security objectives into the report data set.
- Map security objectives, both TOE-specific and from the Knowledge Base, to environmental considerations. This mapping is necessary in order to trace security objectives back to the applicable IT security environmental considerations.

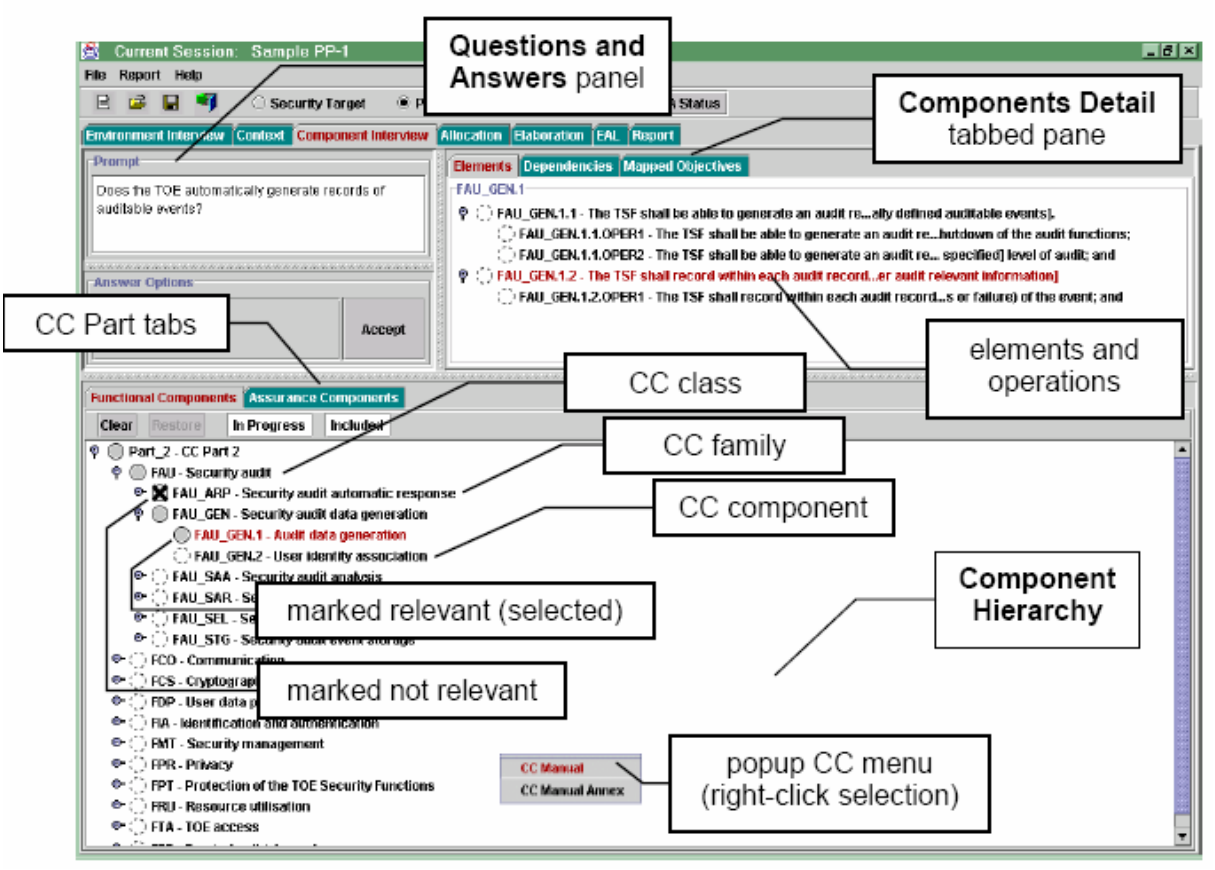
Keep in mind that environmental considerations and security objectives can be part of the reportdata set without being part of the report.



3.5 Component Interview Tab

The main purpose of the **Component Interview** interface is to help you identify CC components that are relevant to your security objectives. It provides structured access to the CC functional and assurance classes, families, and components. In addition, you can display the CC text itself for each class, family, and component.

Like the **Environment Interview** interface, the **Component Interview** interface is made up of three interface components. The **Prompt** panel shows you the question associated with the selected class, family, or CC component. The **Component Detail** tabbed pane gives you information about the selected CC component: the elements that comprise it, its dependencies, and security objectives to which it has been mapped. The **Component Hierarchy** shows the structure of the interview, what CC component is currently selected, and the responses you have entered.

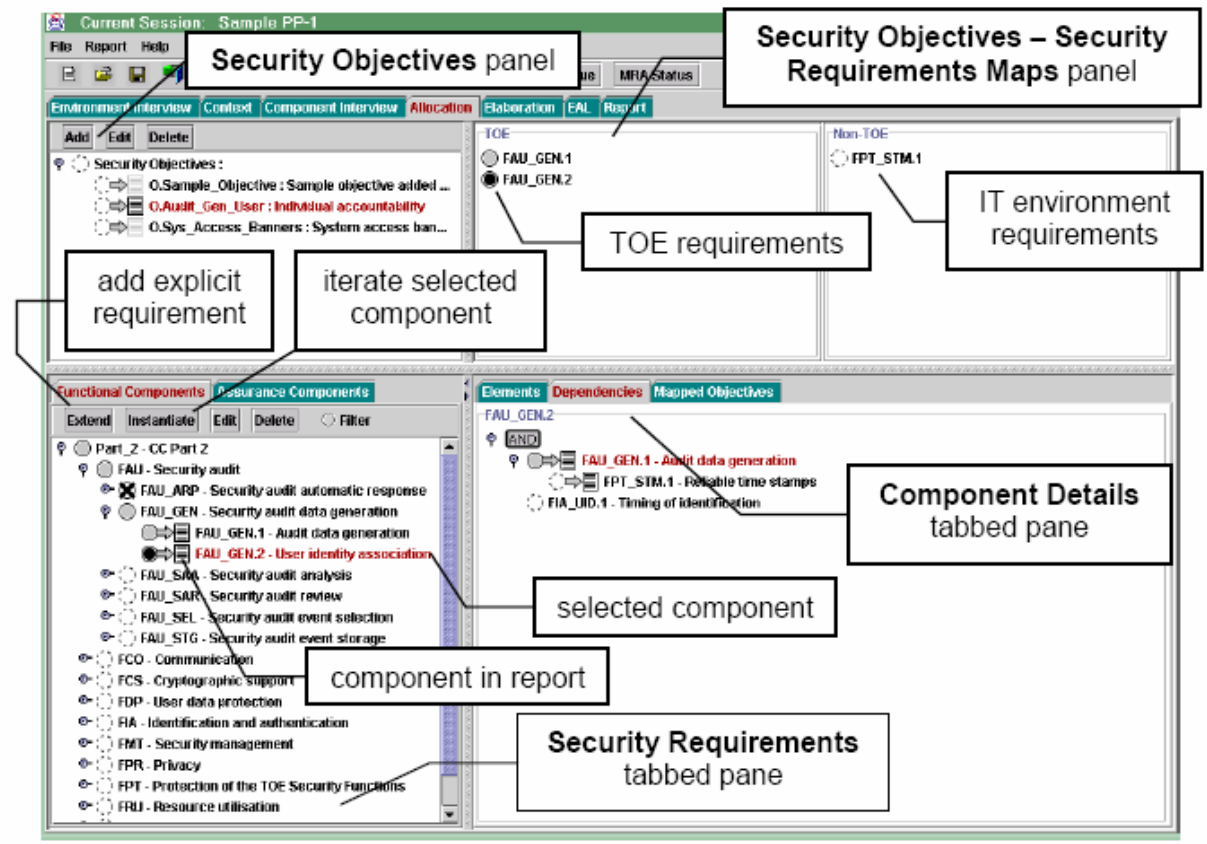


3.6 Allocation Tab

The main purpose of the **Allocation** interface is to enable you to map components to security objectives. (See *Reference Manual*: Allocation.) This mapping is necessary in order to trace security objectives back to the IT security environment.

For the selected security objective, you can map a component to the TOE, which makes that objective an objective for the TOE. You can map the component to the Non-TOE, which makes that objective an objective for the environment. In either case, mapping a component to a security objective makes both the component and security objective part of the report. Keep in mind that security objectives and components can be part of the report data set without being part of the report.

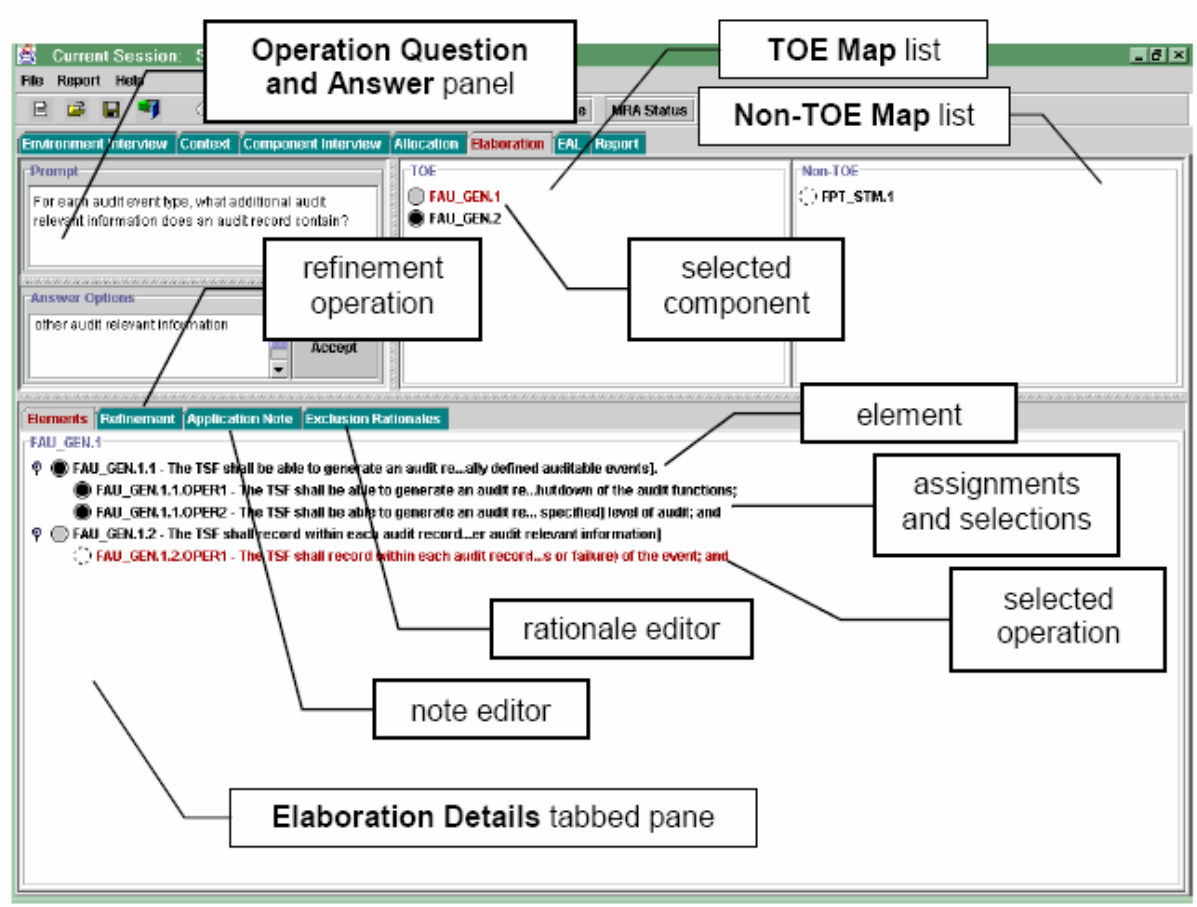
In addition, the **Allocation** interface lets you modify the hierarchy of components. You may apply the CC operation of iteration to the selected component in order to use that component more than once with varying operations. You may write explicit statements of IT requirements not found in the CC.



3.7 Elaboration Tab

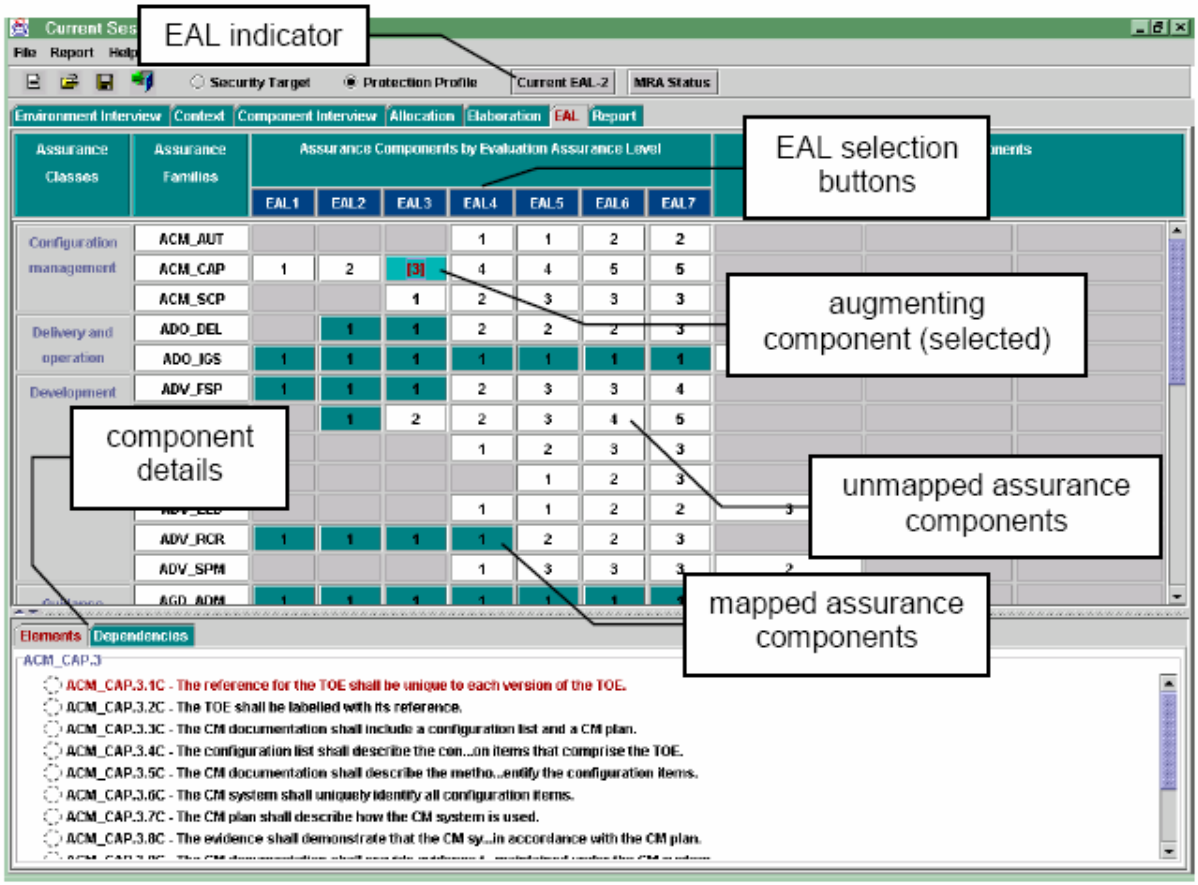
The purpose of the **Elaboration** interface is to provide you with the means to specialize CC components into security requirements specific to your TOE. The interface contains the **Elaboration Details** tabbed pane and each tab presents a different aspect of specialization.

- The **Elements** tab presents interview questions you can use to complete the assignments and selections of the selected component.
- The **Refinement** tab has an editor for applying the refinement operation.
- With the **Application Note** tab, you can add informative notes to accompany the selected component.
- Finally, the **Exclusion Rationales** tab lets you add rationale to justify why a component that is generally needed to meet CC dependencies is not necessary for your specific TOE.



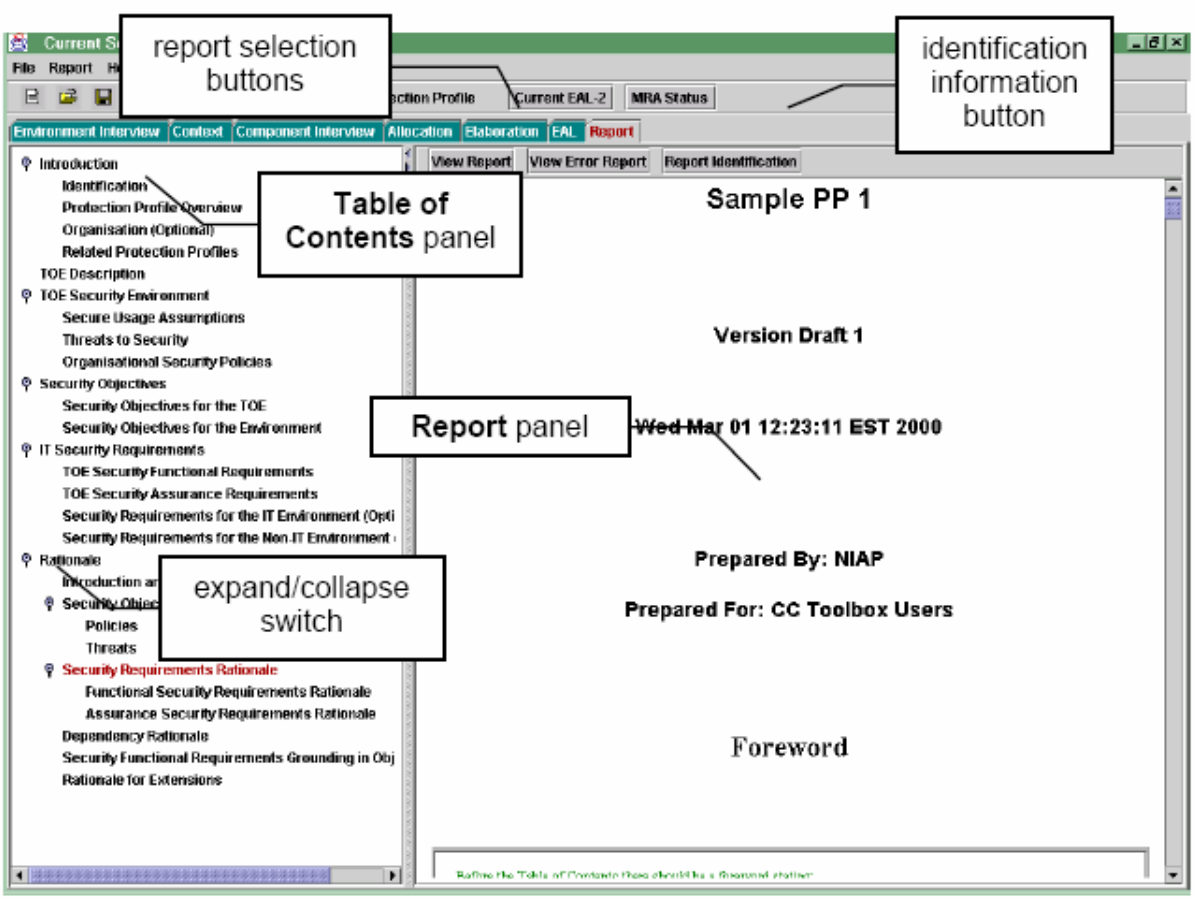
3.8 EAL Tab

The purpose of the **EAL** interface is to let you choose an Evaluation Assurance Level (EAL) for your TOE. It shows which assurance security requirements have been mapped to security objectives and provides details about the selected component.



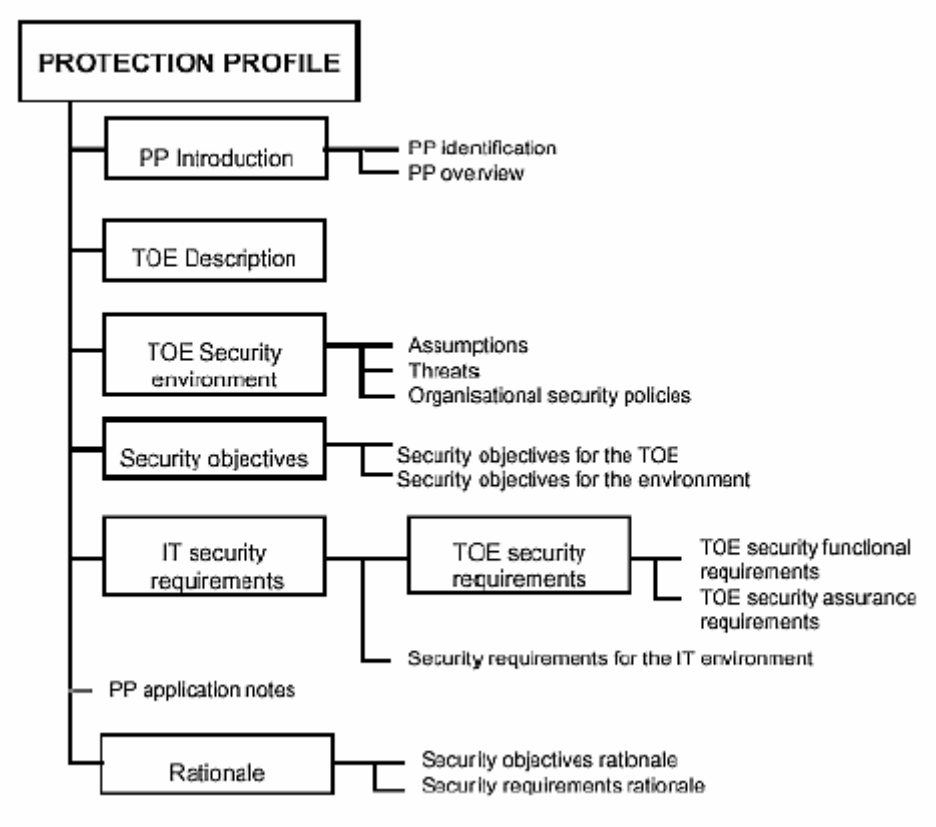
3.9 Report Tab

The main purpose of the **Report** interface is to let you view your report. In addition, you can use the **Report** interface to enter report identification information and to view a list, the so-called error report, of warnings and informational messages about the contents of the report. Remember that the report is not the same as the report data set. An environmental consideration in the report data set appears in the report only if a security objective has been mapped to it. Likewise, a security objective appears in the report only if a component has been mapped to it.



4 Getting Started

The content of a PP is specified in the CC, specifically in Annex B of Part 1 and the APE class in Part 3. Figure B.1 of that annex shows the PP content and is reproduced here.



Briefly, the PP **Introduction** identifies the product. The **TOE Description** provides context for evaluation of the product or system. The **TOE Security Environment** identifies the security concerns. It describes the context in which the TOE is intended to be used.

The **Security Objectives** are the intended response to the security concerns. Security objectives are intended to counter the threats and address the policies and assumptions in the TOE Security Environment.

The **IT Security Requirements** are an elaboration of the security objectives. You use CC component to state your security requirements. The CC defines both functional components (in Part 2) and assurance components (in Part 3). You use the security functional components to express the security functions you require in your product or system. You use the security assurance components to express the requirements for assurance that those security functions are implemented correctly. Finally, you use the operations defined in the CC to tailor the CC components to be specific to your TOE.

The **Rationale** is used in evaluation of the PP to support claims that the PP is complete, consistent, and technically sound and that a conformant TOE would be effective in the security environment.

For further and more detailed information see "Touring the CC Toolbox" chapter 4.

5 Frequently Asked Questions

Question: I answered 'Yes' to **Environment Interview** questions, but the corresponding organizational security policies, assumptions, and threats don't appear in the report. Why don't the environmental considerations appear in the report?

Answer: The CC Toolbox performs consistency checks and does not include in the report information that fails these checks. The CC requires that each threat be countered and have at least one security objective traced to the threat. Similarly, organizational security policies and assumptions must have security objectives traced to them. The CC Toolbox will not include an environmental consideration in the report until you trace a security objective to it. See ***"Touring the CC Toolbox"*** section **8.1 Consistency Checking**, page 115.

Question: I mapped an organizational security policy (or assumption or threat) to a security objective. The policy appears in the report, but not the security objective. Why is the objective missing from the report?

Answer: As in the previous question, security objectives are omitted as a result of failed consistency checks. The CC requires that each security objective for the TOE be met by security requirements and hence have at least one requirement traced to the objective. The CC Toolbox will not include a security objective in the report until you trace a component to it or associate a non-IT security requirement with it. See the next question about security objectives for the non- IT environment and ***"Touring the CC Toolbox"*** Section 8.1 Consistency Checking, page 115.

Question: How do I include in the report a security objective for the non-IT environment that is not met by IT security requirements?

Answer: The CC does not require that security requirements be traced to security objectives for the non-IT environment. However, in the CC Toolbox you must either trace an IT requirement to or associate a non-IT requirement with every security objective that you want included in the report. This is an artifact of the way the CC Toolbox consistency checks were implemented. In this case, the solution is to associate a non-IT requirement with the objective. The text of this requirement may be blank.

Question: I answered 'Yes' to **Component Interview** questions, but the corresponding components don't appear in the report. Why don't they?

Answer: As with the **Environment Interview**, the CC Toolbox performs consistency checks and does not include in the report information that fails these checks. The CC requires that each requirement in a PP be traced to at least one security objective. The CC Toolbox will not include a requirement in the report until you trace it to a security objective. See ***"Touring the CC Toolbox"*** Section 8.1 Consistency Checking, page 115.

Question: I clicked an answer in the **Answer Option** panel, but nothing happened? How do I answer an interview question?

Answer: The CC Toolbox does not record your answer until you click the **Accept** button. When you click the **Accept** button, your answer is added to the report data set and the Toolbox advances the interview to the next appropriate question.

Question: The CC Toolbox doesn't run when I click StartCC from the taskbar. A DOS window opens but the closes immediately. How do I start the CC Toolbox?

Answer: Most often this is a result of installing CC Toolbox version 5.0i over version 4.0. The problem occurs when one of the version 4.0 files, CCToolbox.state, is not overwritten during the installation of version 5.0i. This problem was corrected with CC Toolbox version 5.0j. Downloading and installing the latest version of the Toolbox should address the problem. Alternatively, deleting the CCToolbox.state file should correct the problem for version 5.0i.

Question: How can I change the allocation of a component from the **non-TOE** to the **TOE** or from the **TOE** to the **non-TOE**?

Answer: In CC Toolbox version 6.0, drag the component from the **non-TOE** list to the **TOE** list on the **Allocation** interface. Be advised though that if the component is mapped to more than one security objective, the component will be moved from the **non-TOE** to the **TOE** for *all* the associated security objectives. You can reallocate components from the **TOE** to the **non-TOE** in the same way. In version 5.0, you must first remove all the mappings of the component to the **non-TOE** and then add new mappings to the **TOE**. The mappings must be removed one by one. In both versions, if the TOE satisfies the requirement for some objectives while the non-IT environment satisfies it for others you must iterate the component and allocate the instances appropriately. See the answer to the next question.

Question: How can I allocate the same CC component to both the TOE and the non-TOE simultaneously?

Answer: By allocating a CC component, you are assigning responsibility for implementing that component's security function to either the TOE or to a system in the IT environment. Two distinct systems cannot simultaneously be responsible for implementing one security function. Hence, you cannot allocate the same CC component to both the **TOE** and the **non-TOE**. However, both the TOE and the IT environment may each be responsible for implementing their own version of a security function. In this case, you iterate the CC component for the desired security function. Then you map one instance of the component to the **TOE** and the other instance to the **non-TOE**. Finally, you complete the operations within each instance of the CC component so that each is appropriate to the system to which it has been allocated.

Question: Why do the security objectives appear in an order different from the order in which I entered them?

Answer: The security objectives in the **Security Objectives** list panel are grouped into two groups. The first group contains the TOE-specific security objectives that you entered. The second group contains security objectives incorporated from the CC Profiling Knowledge Base that you mapped to environmental considerations. The security objectives are listed alphabetically within each of these two groups. This ordering of security objectives cannot be changed within the CC Toolbox.

Question: Can I change the fonts used in the CC Toolbox?

Answer: The fonts used in the CC Toolbox cannot be changed. To improve readability, consider changing the resolution of your monitor or using Windows Accessibility options.

Question: The CC Toolbox runs very slowly. Is that normal?

Answer: The CC Toolbox is a memory intensive application. It can take up to two minutes to start on the minimal recommended PC (i.e., a Pentium 133 MHz machine with 64 MB of RAM). Switching between interfaces also takes time on the minimal machine. The performance of the CC Toolbox improves significantly on PC with 128 MB of RAM. If you cannot increase the actual memory of your PC, you may be able to improve performance some by increasing the size of your virtual memory paging file (also called a swap file). The next example illustrates how to call up the Windows help instructions for changing virtual memory paging file size.

Question: How can I prevent the mouse pointer from corrupting the CC Toolbox display?

Answer: The mouse pointer can corrupt the CC Toolbox display on some systems, laptops in particular. To correct the display, turn off mouse trails and use the Windows default pointer scheme. The procedure in ***"Touring the CC Toolbox"*** Figure 10-1 illustrates how to set the Windows pointer scheme for a generic mouse. Your mouse may have additional options.

1. Click **Start** on the Windows Task bar.
2. Move the mouse pointer over **Settings** in the pop up menu, and then click **Control Panel** in the second pop up menu.
3. Double-click **Mouse** in the **Control Panel** window.
4. Click the **Pointers** tab in **Mouse Properties** window.
5. Select **(None)** from the **Scheme** drop down selection list.
6. Click the Motion tab in the Mouse Properties window.
7. Clear the check box for **Mouse Trails**, if present.

Question: How can I view and print the CC Toolbox *Users Guide* and *Reference Manual* outside the CC Toolbox?

Answer: The CC Toolbox program group contains entries for displaying the *Users Guide* and *Reference Manual* as single web pages in your default web browser. You can print each of the documents using your browser's print feature. The procedure for printing the *Users Guide* is described in ***"Touring the CC Toolbox"*** Figure 10-2 and printing the *Reference Manual* is similar.

1. Click **Start** on the Windows Task bar.
2. Move the mouse pointer over **Programs** in the pop up menu
3. Move the mouse pointer over the CC Toolbox program group in the pop up menu, and then click **UsersManual.bat** in the CC Toolbox group pop up menu.

   Your default web browser will start and display the *Users Guide.*
4. Select Print from the web browser File menu, and then click Ok in the Print window.

   The Users Guide prints on your default printer.

Question: No environmental considerations appear in the **Environmental Considerations List** tabbed pane. How do I view the list of environmental considerations?

Answer: There are two possible causes for an empty environmental considerations list. One possible cause is that you did not mark any environmental considerations as relevant on the **Environment Interview** interface and the filter feature is set to display only considerations marked as relevant. If this is the case, click **All** above the list to display all the environment considerations. The filter feature applies independently to the **Assumptions**, **Threats**, and **Policies** lists, and so you may need to click **All** for each list.

Another possible cause is that the report data set does not incorporate the security engineering information from the CC Profiling Knowledge Base. If you are starting a new report data set, click New in the File menu. From the **Predefined Environment List** window, select **DKV5-0-0** to incorporate the standard version of the Knowledge Base information into your report data set. If you report data set is from an earlier version of the CC Toolbox and you want to incorporate CC Profiling Knowledge Base information into it, then create a new report data set in version 5 and cut and paste the information from the old data set into the new one.

6 Examples

Example Add A Non-IT Requirement

1) Click the **Context** tab in the **Top-Level** interface view.

   The **Context** interface appears with the **Security Objectives** panel in the upper left.

   The next few steps add a security objective for the non-IT environment. This objective demonstrates the CC Toolbox features and is not intended as an example of good practice. (See "Add a Security Objective" on page 54 for more details.)

2) Click the **Add** button in the **Security Objectives** panel

   The **Security Objectives Add-Edit** window appears.

3) Click the **Identifier** text field, and then type Physical_Security

4) Click the **Descriptive Name** text field, and then type Physical protection procedures

5) Click the **Description** text field, and then type Implement procedures to protect the TOE from unauthorized physical modification.

6) Click the **Selection Guidance** text field, and then type This is a security objective for the non-IT environment.

7) Click the **Implementation Application** text field, then type No IT requirements should be associated with this security objective.

8) Click **Ok**.

   The **Security Objectives Add-Edit** window closes and **O.Physical_Security** appears as the selected objective in the **Security Objectives** list.

9) Right-click **O.Physical_Security** in the **Security Objectives** list.

   The **View Detail** button pops up.

10) Click the **View Detail** button.

    The **Security Objectives Detail** window appears. It contains three tabs, one of which is labeled **Non-IT**.

11) Click the **Non-IT** tab.

    The **Non-IT** text editor appears.

12) Click in the **Non-IT** text editor and type a single space.

    You also have the option of entering a requirement for the non-IT environment. Any text you enter appears in Section 5.4 Security Requirements for the Non-IT Environment (Optional) of the report.

13) Click the **Accept** ( ) to insert the text into the report.

There is no change in the display. However, the changes you make in the **Non-IT** text editor do not become part of the report data set until you click the **Accept** button.

14) Click the Windows close icon (×) in the upper right corner of the **Security Objectives Detail** window.

The **Security Objectives Detail** window closes. The icon for **O.Physical_Security** changes to showing that a non-IT requirement is associated with the objective. **O.Physical_Security** will now appear in Section 4.2 Security Objectives for the Environment of the report.

Example Accessing Windows Help

1) Click the **Start** button on the task bar.

A menu pops up.

2) Click **Help** on the pop-up menu.

A **Help Topics** dialog box appears.

3) Click the **Index** tab in the **Help Topics** dialog.

4) Type swap file in the top text field.

The list of topics scrolls to the **swap file** topic.

5) Click the **Display** button.

6) A Windows Help dialog box appears. Follow the instructions to change the size of the virtual memory paging file.

Radio Commander Protection Profile

Version 1.0

Prepared By:
Michael Stumpf

Prepared For:
Siemens CT IC CERT

21.01.2005

Foreword

Die Siemens Abteilung CT IC CERT evaluiert IT-Produkte auf potentielle Schwachstellen. Im Rahmen meiner Diplomarbeit soll für Siemens CERT der Einstieg in die Evaluierung anhand von Common Criteria vorbereitet werden, so dass zukünftige Evaluierungen auf diesem internationalen Standard durchgeführt werden können. Anhand eines bereits - nicht nach Common Criteria - evaluierten IT-Produkts, dem Radio Commander, wurde hier ein Protection Profile erstellt, anhand diesem die Unterschiede zur herkömmlichen Zertifizierungsweise nachvollzogen werden können. Das Protection Profile soll darüber hinaus eine Basis für weitere Evaluierungen von IT-Produkten darstellen und orientiert sich daher an einem häufig verwendeten Systemkontext.

Kommentare zum Protection Profile sind an die Abteilung Siemens CT IC CERT zu richten. Ansprechpartner sind Sven Lehmberg und Robert Ingruber.

Das Protection Profile liegt in der Version 1.0 vor.

Table Of Contents

1 - Introduction
1.1 - Identification
1.2 - Protection Profile Overview
1.3 - Organisation (Optional)
1.4 - Related Protection Profiles
2 - TOE Description
3 - TOE Security Environment
3.1 - Secure Usage Assumptions
3.2 - Threats to Security
3.3 - Organisational Security Policies
4 - Security Objectives
4.1 - Security Objectives for the TOE
4.2 - Security Objectives for the Environment
5 - IT Security Requirements
5.1 - TOE Security Functional Requirements
5.2 - TOE Security Assurance Requirements
5.3 - Security Requirements for the IT Environment (Optional)
5.4 - Security Requirements for the Non-IT Environment (Optional)
6 - Rationale
6.1 - Introduction and TOE Description Rationale (Optional)
6.2 - Security Objectives Rationale
6.2.1 - Policies
6.2.2 - Threats
6.3 - Security Requirements Rationale
6.3.1 - Functional Security Requirements Rationale
6.3.2 - Assurance Security Requirements Rationale
6.4 - Dependency Rationale
6.5 - Security Functional Requirements Grounding in Objectives
6.6 - Rationale for Extensions

List of Tables

Table - 5-1 Assurance Requirements: EAL (2)
Table - 6-1 Mapping the TOE Security Environment to Security Objectives
Table - 6-2 Tracing of Security Objectives to the TOE Security Environment
Table - 6-3 Functional Component to Security Objective Mapping
Table - 6-4 Functional and Assurance Requirements Dependencies
Table - 6-5 Requirements to Objectives Mapping

Conventions and Terminology

Conventions

Jedes Computersystem, das an ein Rechenzentrum oder verteiltes Netzwerk angeschlossen ist, soll Sicherheitsleistungen enthalten, die einem akzeptierten Sicherheitsstandard entsprechen oder darüber hinausgehen.

Terminology

Dieses Dokument benutzt die Terminologie der im Vorfeld der internationalen Norm ISO/IEC 15408 „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" veröffentlichten „Common Criteria for Information Technology Security Evaluation" in der Version 2.1 und deren vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellten deutschsprachigen Übersetzung. Aus Gründen der Übersichtlichkeit wird der Begriff „Common Criteria" in diesem Dokument als einheitliche Bezeichnung für diese Referenzdokumente verwendet. Da dieses Schutzprofil Gesamtsysteme beschreibt, wurde der sonst übliche Begriff des Evaluationsgegenstandes (EVG) oft durch den Begriff „System" (eigentlich IT-System) ersetzt. die beiden Begriffe können in diesem Schutzprofil austauschbar verwendet werden.

Da das Protection Profile mit der "CC Toolbox" erstellt wurde und diese standardmäßig die englischen Bezeichnungen verwendet, findet ein ineinander übergehender Wechsel zwischen der englischen und deutschen Sprache statt.

1 - Introduction

Das hier vorgelegte Schutzprofil "Radio Commander" zur Anwendung im Rahmen der Common Criteria wurde mit der Zielsetzung erstellt, grundlegende Sicherheitsanforderungen für die Entwicklung, den Betrieb und die Beschaffung aller IT-Systeme einer Radio Commander Infrastruktur, zu definieren.

Entsprechend der oben formulierten Ziele wendet sich dieses Schutzprofil an verschiedene Zielgruppen:

Mitarbeiter von Siemens CT IC CERT
Die Mitarbeiter von Siemens CT IC CERT können mit diesem Schutzprofil vorhandene IT-Systeme bezüglich ihrer Sicherheit bewerten, sowie Vorgaben für die Entwicklung, den Betrieb und die Beschaffung von IT-Systemen definieren.

Hersteller der zu evaluierenden Produkte
Hersteller können anhand des Schutzprofils ihre eigenen IT-Produkte bewerten und damit erkennen, wie sie ihre Produkte den Sicherheitserfordernissen von Siemens CT IC CERT optimal anpassen können.

1.1 - Identification

Title: Radio Commander

Authors: Michael Stumpf

Vetting Status: PP created

CC Version: 2.1 Final

General Status: Working State

Registration: None

Keywords: Common Criteria

1.2 - Protection Profile Overview

Das vorliegende Schutzprofil definiert einen Satz grundlegender Sicherheitsanforderungen zur Absicherung von IT-Systemen, wie sie typischerweise in einer Radio Commander Infrastruktur zum Einsatz kommen. Das Schutzprofil kennzeichnet dabei die Sicherheitsanforderungen an ein IT-Gesamtsystem, welches aus Arbeitsplatzrechnern, Servern, Hosts und den sie verbindenden Netzkomponenten und der zum Betrieb der Anwendungen notwendigen Software bestehen kann.

Dieses Schutzprofil ist daher auf Systeme anwendbar, die sich aus Hardwarekomponenten, Betriebssystemen, system- und anwendungsnaher Software (sog. Middleware) sowie Anwendungsprogrammen zusammensetzen. Die zum Betrieb eines solchen Gesamtsystems erforderliche bauliche, organisatorische und personelle Infrastruktur muss bestimmten Sicherheitsanforderungen genügen, die nicht durch den EVG realisiert werden. Daher werden bestimmte Annahmen über die Betriebsumgebung gemacht, ohne die die Sicherheit des IT-Gesamtsystems nicht gewährleistet werden kann. Diese Annahmen finden sich in Abschnitt 4.1.1. wieder. Die Verfügbarkeit der Informationen muss weitestgehend gewährleistet sein, insbesondere sind keine unbemerkten und nicht wieder herstellbaren Verluste von geschäfts- und sicherheitsrelevanten Daten tolerierbar.

Systeme, die dem Radio Commander Schutzprofil genügen, sind in der Lage, Zugriffe auf die von ihnen verwalteten Informationen zu kontrollieren, bei der sowohl Zugriffe einzelner Benutzer und Benutzergruppen auf Objekte, die die Informationen enthalten, auf der Grundlage der Ihnen erteilten Zugriffsrechte, als auch Zugriffe einzelner Benutzer auf anwendungskontrollierte Objekte und Funktionen auf der Basis der von Ihnen ausgeübten Rollen möglich sind.

Das Radio Commander Schutzprofil bietet einen Schutz, der für eine Umgebung angemessen ist, in der der Zugriff auf Informationen und Systemressourcen auf dazu berechtigte Benutzer beschränkt werden muss. Dabei sind die Benutzer im Rahmen der Ihnen zugeteilten Rechte als vertrauenswürdig anzusehen. Dies gilt insbesondere auch für den Umgang der Benutzer mit den Informationen, deren Dateneigentümer sie sind. Es ist jedoch erforderlich, sie für jede ihrer Aktionen jederzeit zur Verantwortung ziehen zu können. Siemens CERT fordert mit dem Radio Commander Protection Profile daher eine Reihe von Schutzmechanismen. Zu diesen Schutzmechanismen gehören neben der oben spezifizierten Zugriffskontrolle die Möglichkeit einer starken Authentisierung sowie die Möglichkeit einer umfassenden Protokollierung und Beweissicherung. Von anderen Schutzprofilen unterscheidet sich Radio Commander dadurch, dass es Sicherheitsanforderungen für die Betrachtung von Gesamtsystemen und nicht für einzelne Komponenten formuliert; neben einer rollenbasierten Zugriffskontrolle eine benutzerbestimmte

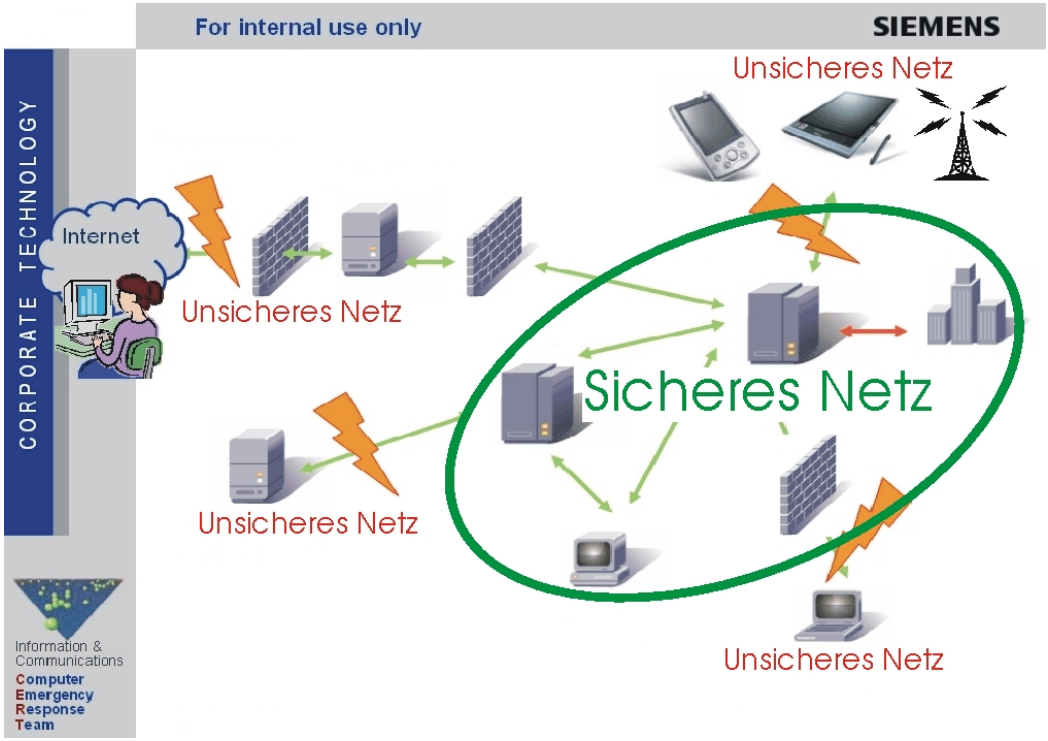
Zugriffskontrolle unter der Voraussetzung vertrauenswürdige Dateneigentümer toleriert; Anforderungen und Ergebnisse bezüglich der IT-Sicherheit berücksichtigt, die von den Erfahrung bisheriger Evaluierungen von IT-Systemen im Rahmen von Siemens basieren.

1.3 - Organisation (Optional)

Die geforderte Stärke der Sicherheitsfunktionen für dieses Schutzprofil ist SoF-mittel. Dies ist die für IT-Systeme von Siemens CERT geforderte Sicherheitsstufe, die dessen potentielle Angriffsszenarien abdeckt. Die Stufe „SoF-hoch" bleibt Systemen vorbehalten, die vor Angreifern mit außerordentlich umfangreichen Ressourcen geschützt werden müssen.

2 - TOE Description

Das Radio Commander Protection Profile beschreibt Sicherheitsanforderungen an IT-Gesamtsysteme für verschiedene Einsatzszenarien, die sich aus Hardwarekomponenten, Betriebssystemen, system- und anwendungsnaher Software sowie Anwendungsprogrammen zusammensetzen.



Mögliche „Systeme" werden in der obigen Abbildung gezeigt. Das Sichere System (innerhalb des Kreises dargestellt) fasst jeweils mehrere Einzelkomponenten zu einem Teilsystem zusammen, welches Gegenstand einer Sicherheitsbetrachtung sein könnte. Auch die Unsicheren Netze könnten Teilsysteme darstellen, werden aber im Folgenden nicht als solche betrachtet. Jedes dieser Teilsysteme kann in einer Sicherheitsbetrachtung als abgeschlossenes, von den restlichen Teilsystemen unabhängiges System angesehen und bezüglich seiner Sicherheitsfunktionen und seiner Vertrauenswürdigkeit bewertet werden. Zusammengenommen bilden alle Teilsysteme jedoch ein Gesamtsystem, das die IT-Dienstleistungen für die Organisation erbringt und das in seiner Gesamtheit die Sicherheitspolitik der Organisation umsetzt. Das Gesamtsystem soll bestimmten Sicherheitsanforderungen genügen. Dazu ist jeweils zu spezifizieren, welche Sicherheitsfunktionen in welchen Teilsystemen erbracht werden. Es ist davon auszugehen, dass keines der Teilsysteme in der Lage ist, die in dem vorliegenden Schutzprofil

beschriebene Sicherheitsfunktionalität ohne die Mitwirkung anderer Teilsysteme zu erbringen.

Folgende Anforderungen werden an das System gestellt:

- Die **Integrität** für Daten während der Übertragung ist als sehr wichtig einzustufen.
- Die **Verfügbarkeit** ist ebenso wichtig und soll vor allem durch Systemalarm-Meldungen und nicht durch Redundanz umgesetzt werden.
- Die **Vertraulichkeit** muss gegeben sein. Vor allem für Passwörter, weniger für die Kommunikation und die restlichen Daten.
- An die Verbindlichkeit werden geringe Anforderungen gestellt
- **Systeme innerhalb des Sicheren-Netzes** (auch Sichere Domäne genannt) können als **vertrauenswürdig** angenommen werden.
- Die Kommunikation mit **Systemen außerhalb der Sicheren Domäne** wird als **nicht vertrauenswürdig** angenommen.

3 - TOE Security Environment

Im sicheren System bzw. sicheren Netz kann vorausgesetzt werden, dass die **Administratoren vertrauenswürdig** und geschult sind. Weiterhin kann davon ausgegangen werden, dass die **Benutzer** im Wesentlichen die **Sicherheitsfunktionen** des Systems **kennen**.

Das sichere System soll **vor unerlaubtem Zugriff** von außen **geschützt** sein.

3.1 - Secure Usage Assumptions

Radio Commander PP konforme Systeme können die hier beschriebene Sicherheit nur bieten, wenn sie korrekt installiert, verwaltet und benutzt werden. Die Betriebsumgebung muss entsprechend der Dokumentation zur Installation, zur Konfiguration, zum Betrieb und entsprechend der Dokumentation für Benutzer und Systemadministratoren, wie sie im Abschnitt zur Vertrauenswürdigkeit (vgl. Abschnitt 6.2) in diesem Schutzprofil beschrieben sind, administriert werden. Zusätzlich werden die nachfolgenden Annahmen vorausgesetzt, um die Sicherheit gewährleisten zu können, die dieses Schutzprofil beschreibt.

Annahmen zur Betriebsumgebung
Radio Commander PP konforme IT-Systeme werden in Umgebungen eingesetzt, in denen eine Kontrolle über die physikalischen Einsatzbedingungen der einzelnen Systemkomponenten gegeben ist. Es gelten hierzu folgende Annahmen:

A.Zutritt Einige, jedoch nicht notwendigerweise alle Betriebsmittel des Systems, einschließlich der Arbeitsplätze, befinden sich innerhalb kontrollierter Räumlichkeiten, zu denen nicht befugten Personen der Zugang verwehrt wird.

A.MatSchutz Sämtliche Systemkomponenten, die wesentlich zur Durchsetzung der Sicherheitspolitik sind und die nicht selbst über Vorrichtungen zum Schutz vor unbefugten materiellen Eingriffen und Modifikationen verfügen, sind durch geeignete materielle Maßnahmen vor Eingriffen und Modifikationen durch unbefugte Dritte geschützt.

Annahmen zum Bedienungspersonal
Folgende Annahmen gelten für die personelle Infrastruktur:

A.Admin Es gibt eine oder mehrere ausgebildete Personen, die das System verwalten, einschließlich der Sicherheit der darin verarbeiteten Informationen und der Zuweisung der Betriebsmittel. Diese Personen sind

im Rahmen der ihnen übertragenen Aufgaben als vertrauenswürdig zu betrachten.

A.Benutzer Die Benutzer sind für die ihnen übertragenen Aufgaben ausreichend geschult, um die Sicherheitsfunktionen des Systems, soweit sie von ihnen benutzt werden, korrekt und in Übereinstimmung mit der Sicherheitspolitik anzuwenden.

Annahmen zu Kommunikationsverbindungen

Das Protection Profile geht davon aus, dass die einzelnen verteilten Komponenten des IT-Systems miteinander vernetzt sind. Es werden dabei keine Annahmen über die von den Netzkomponenten selbst zur Verfügung gestellten Sicherheitsmechanismen gemacht. Die für die Sicherung der Übertragung spezifizierten Anforderungen können auf unterschiedlichen Ebenen erbracht werden. Allerdings werden folgende Annahmen für Verbindungen des Systems zu externen Systemen getroffen:

A.Partner Andere Systeme, mit denen ein Radio Commander PP konformes System kommuniziert, unterliegen der gleichen administrativen Kontrolle und werden unter der gleichen Sicherheitspolitik betrieben wie das Radio Commander PP konforme System selbst. Damit werden alle verbundenen Systeme zu vertrauenswürdigen Teilsystemen und erfüllen insgesamt das Radio Commander Protection Profile. Verbindungen bestehen nur zu Systemen innerhalb einer eigenen Sicherheitsdomäne. Z.B das Sichere Netz.

3.2 - Threats to Security

Ein Radio Commander PP konformes System muss die Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit (im Sinne von Authentizität und Nachvollziehbarkeit) der von ihm verarbeiteten Informationen gewährleisten. Nachfolgende aufgeführte Bedrohungen müssen abgewehrt werden.

Vom EVG abzuwehrende Bedrohungen
Dieser Abschnitt beschreibt die Bedrohungen, die das System aufgrund seiner Sicherheitsfunktionen selbst erkennen und abwehren kann.

B.Zugang Personen erhalten logischen Zugang zum System, obwohl sie dazu nicht befugt sind. Es muss angenommen werden, dass solche Personen unterschiedlichste Fähigkeiten im Umgang mit dem System besitzen. Personen können eher zufällig aus Neugier oder auch in Kenntnis des Wertes der vom System gespeicherten und verarbeiteten Informationen versuchen, Zugang zum System zu erlangen. Dabei können ihnen Ressourcen in unterschiedlichem Umfang zur Verfügung stehen.

B.Zugriff Personen erhalten Zugriff auf Informationen in einem Zugriffsmodus, der nicht erlaubt ist. Es muss angenommen werden, dass solche Personen unterschiedlichste Fähigkeiten im Umgang mit dem System besitzen. Obwohl den Benutzern ein gewisses Maß an Vertrauen entgegengebracht wird, die ihnen erteilten Zugriffsrechte nicht zu missbrauchen, stellt der Wert der im System verarbeiteten und gespeicherten Informationen unter Umständen einen ernstzunehmenden Anreiz für die Benutzer dar, sich in unberechtigter Art und Weise Zugriff auf diese Informationen zu verschaffen.

B.Fehler Es können Fehler in einzelnen Systemkomponenten entstehen. Fehler in einzelnen Systemkomponenten können aus dem Nichtvorhandensein von Sicherheitsfunktionen bzw. aus der fehlerhaften Implementierung von Sicherheitsfunktionen resultieren. Benutzer oder externe Angreifer können solche Fehler, die sie entweder durch zufällige Entdeckung oder durch systematisches Suchen gefunden haben und zur Ausübung von Rechten ausnutzen, die ihnen nicht zustehen würden.

B.Absturz Der sichere Betriebszustand des Systems geht bei schweren Ausnahmefehlern verloren. Durch Systemabstürze aufgrund schwerwiegender Ausnahmefehler kann die Integrität der Sicherheitsdaten des Systems unbemerkt verloren gehen. Bei Wiederanlauf des Systems ist das System dann unter Umständen nicht mehr in der Lage, die Sicherheitspolitik des Systems korrekt umsetzen.

B.Verfügbarkeit Berechtigte Benutzer können auf die Informationen und Ressourcen des Systems nicht zugreifen. Durch die große Abhängigkeit eines Unternehmens von seinen Informations- und

Kommunikationssystemen ist es für den Geschäftserfolg des Unternehmens unerlässlich, dass Informationen stets dann verwendet und bearbeitet werden können, wenn dies durch die betroffenen Geschäftsprozesse erforderlich ist. Nichtverfügbarkeit oder eingeschränkte Verfügbarkeit von Informationen und Diensten kann durch verschiedenste Umstände hervorgerufen werden.

B.Beweis Sicherheitsrelevante Ereignisse werden nicht aufgezeichnet oder können dem Benutzer, der sie ausgelöst hat, nicht eindeutig zugeordnet werden. Eine sachgemäße Kontrolle der Sicherheit des Systems kann nur dann erfolgen, wenn sicherheitsrelevante Ereignisse erkannt und aufgezeichnet werden. Es muss stets möglich sein, solche Ereignisse den Benutzern, die sie ausgelöst haben, eindeutig zuzuordnen. Auch die Aufzeichnung dieser sicherheitsrelevanten Ereignisse muss vor Manipulation, Zerstörung und unerlaubtem Zugriff geschützt werden. Wenn diese Voraussetzungen nicht erfüllt sind, kann eine angemessene Reaktion auf Attacken gegen das System nicht mehr gewährleistet werden.

B.Manipulation Manipulation sicherheitsrelevanter Mechanismen ist möglich. Die Systemmodule und Daten, die für die Durchsetzung der Sicherheitspolitik des Systems verantwortlich sind, können umgangen oder manipuliert werden. Dadurch kann die Integrität der Sicherheitsmechanismen verletzt und die Durchsetzung der Sicherheitspolitik des Systems nicht mehr gewährleistet sein.

B.Erkennen Ereignisse während des Betriebes, die die Sicherheit des Systems verletzen, werden nicht rechtzeitig erkannt. Diese Bedrohung besteht aufgrund der menschlichen Schwäche der Systemadministratoren, auftretende Probleme im Zusammenhang mit der Systemsicherheit nicht zuverlässig erkennen zu können. Dies kann dazu führen, dass beim Nichterkennen von aufgetretenen Sicherheitsproblemen das System in einem unsicheren Zustand weiter betrieben wird und die Systemadministratoren weiterhin davon ausgehen, dass sich das System in einem sicheren Zustand befindet. Ausgelöst werden kann das Nichterkennen von Sicherheitsproblemen z.B. durch das Nichterkennen von Meldungen, oder durch fehlende, unverständliche oder unvollständige Meldungen.

Von der Betriebsumgebung abzuwehrende Bedrohungen

Die nachfolgend aufgeführten Bedrohungen müssen abgewehrt werden, um die Sicherheit eines Radio Commander PP konformen Systems zu gewährleisten. Da das System sie jedoch nicht selbst abwehren kann, muss in der Betriebsumgebung Vorsorge für ihre Abwehr getroffen werden. Die Abwehr dieser Bedrohungen ist nicht Bestandteil der Sicherheitsfunktionalität, die ein Radio Commander PP konformes System erbringt.

B.Installation Das System kann in einem unsicheren Zustand ausgeliefert und installiert werden. Wurde ein Radio Commander PP konformes System in einem unsicheren Zustand geliefert oder installiert, können sicherheitsrelevante Funktionalitäten des Systems unter Umständen nicht aktiv sein oder durch Benutzer umgangen bzw. ausgeschaltet werden. Der sichere Betrieb des Radio Commander PP konformen Systems kann dann nicht mehr gewährleistet werden.

B.Rollen Die Definition und die Zuweisung von Rollen geschieht so, dass die Sicherheitspolitik verletzt wird. Durch die Definition einer Vielzahl unterschiedlicher Rollen im Rahmen eines Rollenkonzeptes können Rechtekombinationen für einzelne Benutzer entstehen, die im Widerspruch zur Sicherheitspolitik des Unternehmens stehen. Jede einzelne Rolle kann dabei für sich allein die Anforderungen der Sicherheitspolitik erfüllen, jedoch können durch Zuweisung mehrerer Rollen an einen Benutzer kombinierte Rechte dieses Benutzers entstehen, die über die Rechte der einzelnen Rollen hinausgehen und damit die Sicherheitspolitik bei Ausübung dieser Rechtekombinationen verletzen. Ebenso können Benutzer solche Rollen zugewiesen bekommen, die sie aufgrund ihrer tatsächlichen Pflichten nicht einnehmen dürften. Dadurch können Benutzer Zugriff auf Bereiche des Systems erhalten, für die sie aufgrund ihrer Funktion im Unternehmen nicht berechtigt sind. Ein besonderes Problem stellt die Möglichkeit einer Zuweisung von sich gegenseitig ausschließenden Rollen an einen Benutzer dar.

B.Gewalt Durch äußere Gewalteinwirkung können sicherheitskritische Komponenten des Systems manipuliert oder außer Funktion gesetzt werden. Werden Komponenten des Radio Commander PP konformen Systems durch äußere Gewalteinwirkung ausgeschaltet oder in ihrer Funktion beeinträchtigt, können die darauf aufbauenden, im wesentlichen auf logischen Kontrollen basierenden Sicherheitsfunktionen des Systems ihre Leistungen nicht mehr oder nur in vermindertem Umfang erbringen. Nach einer erfolgreichen Manipulation der sicherheitskritischen Komponenten kann ein sicherer Betrieb des Radio Commander PP konformen Systems nicht mehr sichergestellt werden.

3.3 - Organisational Security Policies

In diesem Protection Profile werden keine speziellen Sicherheitspolitiken aufgeführt.

Zur Abwehr der spezifizierten Bedrohungen ergeben sich die nachfolgenden Sicherheitsziele, die von einem Radio Commander PP konformen System und seiner Betriebsumgebung erfüllt werden müssen.

Die Zusammenhänge zwischen Bedrohungen und Sicherheitszielen werden im Abschnitt 6.2 aufgezeigt.

5.1 Sicherheitsziele für den EVG

Z.Zugang Das System unterbindet jeglichen logischen Zugang von unbefugten, d.h. nicht berechtigten Personen bzw. Kommunikationspartnern zum System. Dies kann beispielsweise bedeuten, dass sich jeder Benutzer identifizieren und authentisieren muß, bevor der logische Zugang zum System gewährt wird.

Z.Zugriff Das System verhindert, daß Benutzer Zugriff zu Informationen oder Ressourcen des Systems erhält, für die er aufgrund seiner Rolle oder seiner individuellen Berechtigung keine Zugriffsrechte besitzt.

Z.Archiv Das System ermöglicht, Programme inklusive Dokumentation und die dazugehörigen Datenbestände entsprechend den gesetzlichen und geschäftlichen Anforderungen zu archivieren, um so eine Wiederherstellung einer bestimmten Verarbeitungsumgebung und der erforderlichen Dokumentation zu gewährleisten.

Z.Verantwortung Das System stellt sicher, daß alle Benutzer für ihre sicherheitsrelevanten Aktionen zur Verantwortung gezogen werden können. Dies bedeutet, daß das System in der Lage ist,

- alle zur Nachvollziehbarkeit, Beweispflicht und Revisionssicherheit notwendigen Daten fälschungssicher zu erzeugen. Die aufzuzeichnenden Informationen sind anwendungsbezogen festzulegen. Alle zum personen- bzw. rollenbezogenen Nachweis benötigten Informationen sind von Anwendungssystemen zur Verfügung zu stellen.
- alle vom System erfaßten revisionsrelevanten Daten werden im System gesichert abgelegt. Der Zugriff auf diese Daten ist nur besonders priviligierten Personen, z.B. Administratoren oder Auditoren möglich.

Somit werden diese vor unbefugter Manipulation geschützt.

Z.Zeit-Ort Das System kann den Zugang in Abhängigkeit vom jeweiligen Benutzer auf bestimmte Zeitpunkte und Zugangspunkte beschränken.

Z.Umgehung Das System stellt sicher, daß Angreifer mittels vorsätzlich manipulierter oder fehlerhafter Software die Sicherheitsmechanismen des

Systems, unter Berücksichtigung des angenommenen Angriffspotentials, nicht umgehen können.

Z.Fehler Das System enthält keine für Angriffe auf die IT-Sicherheit des Systems ausnutzbaren Schwachstellen, unter Berücksichtigung des angenommenen Angriffspotentials, in Design, Implementierung oder Betrieb.

Z.SysAdmin Das System stellt alle erforderlichen Funktionen für seine Verwaltung durch berechtigte Systemadministratoren zur Verfügung.

Z.Betrieb Das System gewährleistet die fortlaufende korrekte Funktionsweise seiner Sicherheitsfunktionen.

Z.Status Das System gewährleistet jederzeit die Überprüfung seines Sicherheitsstatus durch die dazu befugten Systemadministratoren.

Z.Verfügbarkeit Das System gewährleistet die durchgehende Verfügbarkeit seiner Ressourcen für seine befugten Benutzer.

Z.Zustand Das System bewahrt auch im Fehlerfall einen sicheren Zustand.

Z.Verbindung Das System kann mit vertrauenswürdigen Partnern unter Erhalt der Vertraulichkeit und Integrität der übertragenen Daten kommunizieren.

Z.Software Die auf den Systemen in sicherheitsrelevanten Bereichen zum Einsatz kommende Software ist vertrauenswürdig. Dies wird dadurch erreicht, daß sie methodisch entwickelt, getestet und durchgesehen wurde.

5.2 Sicherheitsziele für die Umgebung

Z.Installation Die für den Betrieb des Systems Verantwortlichen stellen sicher, daß das System in einer Art und Weise ausgeliefert und installiert wird, die die Sicherheit des Systems gewährleistet.

Z.Definition Die Definition und Zuweisung von Rollen und Gruppen erfolgt in Übereinstimmung mit der geltenden Sicherheitspolitik. Aufgaben und die von einem berechtigten Benutzer zu einem bestimmten Zeitpunkt ausgeübte Rolle sind jederzeit klar erkennbar.

Z.Geheim Die Benutzer gewährleisten den Schutz ihrer Authentisierungsgeheimnisse.

Z.Aufbewahrung In der Betriebsumgebung bestehen Möglichkeiten zur Aufbewahrung von Daten, Programmen und Protokollinformationen gemäß den gesetzlichen Regelungen.

Z.KommAdmin Die für den Betrieb des Systems Verantwortlichen stellen sicher, dass keine Verbindungen zu nicht vertrauenswürdigen Systemen die Sicherheit des Systems gefährden.

Z.Zutritt Einige, jedoch nicht notwendigerweise alle Betriebsmittel des Systems, einschließlich der Arbeitsplätze, befinden sich innerhalb kontrollierter Räumlichkeiten, zu denen nicht befugten Personen der Zugang verwehrt wird.

Z.Schutz Sämtliche Systemkomponenten, die wesentlich zur Durchsetzung der Sicherheitspolitik sind und die nicht selbst über Vorrichtungen zum Schutz vor unbefugten materiellen Eingriffen und Modifikationen verfügen, werden durch geeignete materielle Maßnahmen vor Eingriffen und Modifikationen durch unbefugte Dritte geschützt.

Z.Admin Es gibt eine oder mehrere ausgebildete Personen, die das System verwalten, einschließlich der Sicherheit der darin verarbeiteten Informationen und der Zuweisung der Betriebsmittel. Diese Personen sind im Rahmen der ihnen übertragenen Aufgaben als vertrauenswürdig zu betrachten.

Z.Benutzer Die Benutzer sind für die ihnen übertragenen Aufgaben ausreichend geschult, um die Sicherheitsfunktionen des Systems, soweit sie von ihnen benutzt werden, korrekt und in Übereinstimmung mit der Sicherheitspolitik anzuwenden.

Z.Partner Andere Systeme, mit denen ein SIZ-PP-konformes System kommuniziert, unterliegen der gleichen administrativen Kontrolle und werden unter der gleichen Sicherheitspolitik betrieben wie das System selbst.

5 - IT Security Requirements

Es folgt eine detaillierte Auflistung aller Sicherheitskomponenten des Radio Commander Protection Profiles.

5.1 - TOE Security Functional Requirements

5.1.1 - Security audit (FAU)

5.1.1.1 - Security alarms (FAU_ARP.1)

Die TSF müssen

- die Alarmierung eines verantwortlichen Systemadministrators
- eine Vereitelung der Sicherheitsverletzung durch eine der folgenden Aktionen:
  - Herunterfahren des Systems;
  - Sperrung des Zugangspunktes oder Dienstes, über den die potentielle Sicherheitsverletzung erfolgt;
  - Sperrung der Benutzerkennung, von der aus die potentielle Sicherheitsverletzung erfolgt;
  - Entfernen des Subjektes, von dem aus die potentielle Sicherheitsverletzung erfolgt;
  - Entfernen aller Subjekte mit der Benutzerkennung, von der aus die potentielle Sicherheitsverletzung erfolgt;
  - Starten eines Programmes;

bei Erkennung einer potentiellen Sicherheitsverletzung ausführen. ***FAU_ARP.1.1***

5.1.1.2 - Audit data generation (FAU_GEN.1)

The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the not specified level of audit; and
c) other specifically defined auditable events. ***FAU_GEN.1.1***

The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, other audit relevant information ***FAU_GEN.1.2***

5.1.1.3 - User identity association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event. ***FAU_GEN.2.1***

5.1.1.4 - Potential violation analysis (FAU_SAA.1)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. ***FAU_SAA.1.1***

Die TSF müssen zur Überwachung von protokollierten Ereignissen die folgenden Regeln durchsetzen:

Eine Häufung oder Kombination von
- abgewiesenen Anmeldeversuchen innerhalb eines bestimmten Zeitraumes
- abgewiesenen Anmeldeversuchen einer einzelnen Benutzerkennung
- abgewiesenen Anmeldeversuchen von einem einzelnen Zugangspunkt aus
- abgewiesenen Zugriffen auf Objekte innerhalb eines bestimmten Zeitraums
- abgewiesenen Zugriffen auf ein einzelnes Objekt
- abgewiesenen Zugriffen auf Objekte durch eine einzelne Benutzerkennung
- abgewiesenen Zugriffen auf Objekte von einem einzelnen Zugangspunkt aus,

die bekannterweise eine potentielle Sicherheitsverletzung anzeigen, muss erkannt werden. ***FAU_SAA.1.2***

5.1.1.5 - Audit review (FAU_SAR.1)

Die TSF müssen für die befugten Systemadministratoren die Fähigkeit bereitstellen, sämtliche Informationen über protokollierte Ereignisse aus den Protokollaufzeichnungen zu lesen. ***FAU_SAR.1.1***

The TSF shall provide the audit records in a manner suitable for the user to interpret the information. ***FAU_SAR.1.2***

5.1.1.6 - Restricted audit review (FAU_SAR.2)

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. ***FAU_SAR.2.1***

5.1.1.7 - Selectable audit review (FAU_SAR.3)

Die TSF müssen die Fähigkeit der Ausführung von Suchen und Sortieren von Protokolldaten auf Grundlage von
- Benutzerkennungen
- Kennungen eines Subjektes
- Kennungen von Objekten (z.B. Pfadname)
- Zeiträumen
- Ereignissen, die eine Protokollierung ausgelöst haben

bereitstellen. ***FAU_SAR.3.1***

5.1.1.8 - Selective audit (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: object identity user identity subject identity host identity event type ***FAU_SEL.1.1***

5.1.1.9 - Guarantees of audit data availability (FAU_STG.2)

The TSF shall protect the stored audit records from unauthorised deletion. ***FAU_STG.2.1***

The TSF shall be able to prevent modifications to the audit records. ***FAU_STG.2.2***

TSF müssen sicherstellen, dass bei Auftreten einer der folgenden Bedingungen
- Protokollspeicher erschöpft
- Fehler
- Angriff

bis auf eine festgelegte Anzahl von Einträgen, deren Verlust toleriert wird, alle Protokollaufzeichnungen erhalten werden. ***FAU_STG.2.3***

5.1.1.10 - Prevention of audit data loss (FAU_STG.4)

Die TSF müssen, wenn das Protokoll voll ist,
- protokollierbare Ereignisse ignorieren oder
- protokollierbare Ereignisse verhindern, ausgenommen solche,

die von einem autorisierten Benutzer mit besonderen Rechten herbeigeführt werden und einen befugten Systemadministrator über den Überlauf des Protokolls informieren. ***FAU_STG.4.1***

5.1.2 - Communication (FCO)

Comment [1]: Sind das wirklich relevante Punkte? Punkt Verbindlichkeit ist weniger wichtig

5.1.2.1 - Selective proof of origin (FCO_NRO.1)

Die TSF müssen auf Anforderung des Urhebers für
- alle übertragenen Objekte, die über nicht vertrauenswürdige Pfade übermittelt werden
- alle übertragenen Objekte, für die aufgrund von rechtlichen Vorschriften ein Absendernachweis gegenüber einem neutralen Dritten erforderlich werden kann

Urheberschaftsnachweise generieren können. ***FCO_NRO.1.1***

Die TSF müssen die [Zuweisung: Liste der Attribute] des Informationsurhebers den [Zuweisung: Liste der Informationsfelder] der Informationen, auf die sich der Nachweis bezieht, zuordnen können. ***FCO_NRO.1.2***

Die TSF müssen
- dem Absender des Objektes
- dem Empfänger des Objektes
- einem befugten, neutralen Dritten

die Fähigkeit zum Verifizieren des Urheberschaftsnachweises von Informationen unter der Vorgabe von [Zuweisung: Begrenzungen des Urheberschaftsnachweises] bereitstellen. ***FCO_NRO.1.3***

5.1.2.2 - Selective proof of receipt (FCO_NRR.1)

Die TSF müssen auf Anforderung des Urhebers für
• empfangene elektronische Post
• alle empfangenen Objekte, für die aufgrund von rechtlichen Vorschriften ein Empfängernachweis erforderlich ist.
Empfangsnachweise generieren können. ***FCO_NRR.1.1***
Die TSF müssen die [Zuweisung: Liste der Attribute] des Informationsempfängers den [Zuweisung: Liste der Informationsfelder] der Informationen, auf die sich der Nachweis bezieht, zuordnen können. ***FCO_NRR.1.2***

TSF müssen die Fähigkeit zum Verifizieren des Empfangsnachweises von Informationen durch
• den Absender des Objektes
• den Empfänger des Objektes
• einen befugten, neutralen Dritten
unter Vorgabe von [Zuweisung: Begrenzungen des Empfangsnachweises] bereitstellen. ***FCO_NRR.1.3***

5.1.3 - Cryptographic support (FCS)

5.1.3.1 - Cryptographic key generation (FCS_CKM.1)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Radio Commander Standard and specified cryptographic key sizes Standards that meet the following standards. ***FCS_CKM.1.1***

5.1.3.2 - Cryptographic key distribution (FCS_CKM.2)

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method cryptographic key distribution method that meets the following: list of standards. ***FCS_CKM.2.1***

5.1.3.3 - Cryptographic key access (FCS_CKM.3)

Die TSF müssen den Zugriff auf kryptographische Schlüssel für
• die Sicherung von Schlüsseln (cryptographic key backup)
• die Archivierung von Schlüsseln (cryptographic key archival)
• die Hinterlegung von Schlüsseln (cryptographic key escrow)
• das Wiedererlangen von Schlüsseln (cryptographic key recovery)
gemäß einer zugelassenen Zugriffsmethode auf kryptographische Schlüssel durchführen. ***FCS_CKM.3.1***

5.1.3.4 - Cryptographic key destruction (FCS_CKM.4)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method cryptographic key destruction method that meets the following: list of standards. ***FCS_CKM.4.1***

5.1.3.5 - Cryptographic operation (FCS_COP.1)

Die TSF müssen alle kryptographischen Operationen gemäß eines vom ZKA zugelassenen kryptographischen Algorithmus und vom ZKA zugelassener kryptographischer Schlüssellängen durchführen. ***FCS_COP.1.1***

5.1.4 - User data protection (FDP)

5.1.4.1 - Subset access control (FDP_ACC.1)

TSF müssen die benutzerbestimmte Zugriffskontrolle für die Zugriffe von
- allen Subjekten auf
- Objekte im Sinne der benutzerbestimmten Zugriffskontrolle durchsetzen. ***FDP_ACC.1.1***

5.1.4.2 - Security attribute based access control (FDP_ACF.1)

Die TSF müssen die benutzerbestimmte Zugriffskontrolle für Objekte, die auf den folgenden Attributen basieren, durchsetzen:

Subjektattribute:
- die Benutzerkennung des Subjektes
- eine Liste der Gruppen, in denen der Benutzer Mitglied ist
- die Privilegien des Subjekts, soweit vom System unterstützt.

Objektattribute (Zugriffskontrollisten – Access Control Lists (ACLs)):
- eine Liste von Benutzer- und/oder Gruppenkennungen, sowie für jeden Listeneintrag eine Liste der erlaubten Operationen.
- eine Liste von Benutzer- und/oder Gruppenkennungen, für die jeder Zugriff explizit verboten ist

und/oder
- eine Liste von Benutzer- und/oder Gruppenkennungen, sowie für jeden Listeneintrag eine Liste der explizit verbotenen Operationen.

FDP_ACF.1.1

TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist:
- Die Benutzerkennung ist nicht in der Liste der Benutzerkennungen vorhanden, für die der Zugriff explizit verboten ist.
- Keine der Gruppen aus der Liste der Gruppen des Subjekts ist in der Liste der Gruppen vorhanden, für die der Zugriff explizit verboten ist.
- Die (kumulierten) Rechte aus den ACL-Einträgen, die die Benutzerkennung oder mindestens eine der Gruppen aus der Gruppenliste des Subjektes enthalten, beinhalten alle angeforderten Zugriffsrechte. ***FDP_ACF.1.2***

Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf den folgenden zusätzlichen Regeln, explizit autorisieren:
• Zugriffsverweigerung hat Vorrang vor der Gewährung des Zugriffs. Der befugte Systemadministrator darf alle für ihn zugelassenen Operationen auf alle Objekte durchführen. ***FDP_ACF.1.3***

Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf folgenden Regeln:
• Die Benutzerkennung ist in der Liste der Benutzerkennungen vorhanden, für die der Zugriff explizit verboten ist.
• Mindestens eine Gruppe aus der Liste der Gruppen des Subjekts ist in der Liste der Gruppen vorhanden, für die der Zugriff explizit verboten ist.
explizit verweigern. ***FDP_ACF.1.4***

5.1.4.3 - Full residual information protection (FDP_RIP.2)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects. ***FDP_RIP.2.1***

5.1.4.4 - Stored data integrity monitoring and action (FDP_SDI.2)

Die TSF müssen die innerhalb des TSC gespeicherten Benutzerdaten auf unbeabsichtigte (z.B. durch fehlerhafte Speichermedien bedingte) Integritätsfehler bei allen Objekten auf Basis folgender Attribute: [Zuweisung: Benutzerdaten-Attribute] überwachen. ***FDP_SDI.2.1***

Bei Erkennen eines Datenintegritätsfehlers müssen die TSF den Zugriff auf das von diesem Fehler betroffene Objekt mit einem Fehlercode abbrechen. ***FDP_SDI.2.2***

5.1.4.5 - Basic data exchange confidentiality (FDP_UCT.1)

Die TSF müssen die benutzerbestimmte Zugriffskontrolle durchsetzen, um in der Lage zu sein, Objekte vor nichtautorisierter Preisgabe geschützt zu übertragen. ***FDP_UCT.1.1***

5.1.4.6 - Data exchange integrity (FDP_UIT.1)

Die TSF müssen die benutzerbestimmte Zugriffskontrolle durchsetzen, um in der Lage zu sein, Benutzerdaten vor Modifizieren, Löschen, Einfügen und Wiedereinspielen geschützt zu übertragen. ***FDP_UIT.1.1***

Comment [2]: Frage an Sven: Ist das so beim RadioCommander

The TSF shall be able to determine on receipt of user data, whether modification deletion insertion replay has occurred. ***FDP_UIT.1.2***

5.1.5 - Identification and authentication (FIA)

5.1.5.1 - Authentication failure handling (FIA_AFL.1)

Die TSF müssen erkennen, wenn hintereinander mindestens drei misslungene Authentisierungsversuche auftreten, die in Bezug zu
• der Eingabe eines Benutzernamens,
• der Eingabe eines Authentisierungsgeheimnisses,
stehen. ***FIA_AFL.1.1***

Wenn die definierte Anzahl von fehlgeschlagenen Authentisierungsversuchen erreicht oder überschritten wird, müssen die TSF
• einen befugten Systemadministrator benachrichtigen,
• bei wiederholten Fehlversuchen unter einer Benutzerkennung diese Benutzerkennung bis zu einer erneuten Freigabe durch einen befugten Systemadministrator sperren,
• bei wiederholten Fehlversuchen von einem Zugangspunkt diesen Zugangspunkt bis zu einer erneuten Freigabe durch einen befugten Systemadministrator sperren. ***FIA_AFL.1.2***

5.1.5.2 - User attribute definition (FIA_ATD.1)
Die TSF müssen die folgende Liste von Sicherheitsattributen, die zu einzelnen Benutzern gehören, erhalten:
• einen vollen Namen oder andere Informationen, die einen eindeutigen Rückschluß auf die tatsächliche Person bzw. den Kommunikationspartner zulassen
• eine Liste der Gruppen, denen der Benutzer angehört
• eine Liste der Rollen, denen der Benutzer angehört
• die Attribute zur Konfiguration des Systemzuganges
• die Lebensdauer der Kennung
• die erlaubten Login-Zeiten
• den Zeitpunkt des letzten erfolgreichen Logins, den Zeitpunkt des letzten fehlgeschlagenen Logins und die Anzahl der aufeinanderfolgenden fehlgeschlagenen Logins
• eine Liste der erlaubten Zugangspunkte
• die Attribute zur Konfiguration des Authentisierungs-mechanismus:
  - die Attribute des Authentisierungsgeheimnisses
  - die individuellen Attribute für Parameter des Authentisierungsmechanismus.
  - Bei regelmäßig zu ändernden Authentisierungs-geheimnissen wie Passwörtern oder PINs sind dies:
    - der Zeitpunkt der letzten Änderung oder die Anzahl der Änderungen an einem Tag
    - das Verfallsdatum
    - der Zeitpunkt der Warnung über die bevorstehende Änderung
    - eine Liste der zuletzt verwendeten Authentisierungs-geheimnisse.

Comment [3]: Fraglich?

Comment [4]: Fraglich?

Die Länge dieser Liste muss dabei ein Mehrfaches der pro Tag zulässigen Änderungen des Authentisierungsgeheimnisses betragen. ***FIA_ATD.1.1***

5.1.5.3 - Verification of secrets (FIA_SOS.1)

Die TSF müssen einen Mechanismus bereitstellen, um zu verifizieren, dass die Geheimnisse den folgenden Anforderungen

• Neu gewählte Authentisierungsgeheimnisse müssen sich von dem zu diesem Zeitpunkt für diesen Benutzer gültigen Authentisierungsgeheimnis unterscheiden.

• Neu gewählte Authentisierungsgeheimnisse dürfen in der Liste der zuletzt von diesem Benutzer verwendeten Authentisierungsgeheimnisse nicht enthalten sein.

• Bei der Benutzung von Mechanismen für wieder verwendbare Passwörter als Authentisierungsgeheimnis sollen zusätzlich folgende Richtlinien gelten:

- Passwörter müssen eine Mindestlänge von sechs Zeichen haben und sich aus Buchstaben, Ziffern und Sonderzeichen zusammensetzen. Passwörter müssen mindestens ein Zeichen enthalten, das kein Buchstabe ist.
- Triviale Passwörter müssen über Ausnahmelisten vermieden werden können.
- Der Mechanismus zur Passwortüberprüfung muss austauschbar sein.

• Bei Nichterfüllung einer der o.g. Anforderungen wird eine Änderung des zu diesem Zeitpunkt für diesen Benutzer gültigen Authentisierungsgeheimnisses abgewiesen.

entsprechen. ***FIA_SOS.1.1***

5.1.5.4 - User authentication before any action (FIA_UAU.2)

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. ***FIA_UAU.2.1***

5.1.5.5 - Single-use authentication mechanisms (FIA_UAU.4)

Die TSF müssen den Wiedergebrauch von Authentisierungsdaten, die mit dem Authentisierungs-mechanismus „starke Authentisierung" in Beziehung

stehen, verhindern. ***FIA_UAU.4.1***

5.1.5.6 - Multiple authentication mechanisms (FIA_UAU.5)

Die TSF müssen folgende Authentisierungsmechanismen zur Unterstützung der Benutzerauthentisierung bereitstellen:

- „keine Authentisierung"
- „passwortbasierte Authentisierung" oder ein mindestens gleich starker Authentisierungsmechanismus.
- „Starke Authentisierung" nach Anforderung FIA_UAU.4, falls Zugänge nicht-anonymer Benutzer zum System über externe, ungeschützte Leitungen erfolgen.
- „Mehraugen-Prinzip"6
- Zusätzliche Authentisierungsmechanismen, die befugte Systemadministratoren installieren können. ***FIA_UAU.5.1***

Die TSF müssen jede von einem Benutzer angegebene Identität gemäß den folgenden Regeln authentisieren:

- Systeme, die Informationsdienste für anonyme Benutzer zur Verfügung stellen, verwenden für solche anonymen Benutzer den Mechanismus „keine Authentisierung".
- Alle anderen Benutzer verwenden beim Zugang über interne Netze und über geschützte externe Leitungen mindestens den Mechanismus „paßwortbasierte Authentisierung" oder sein Äquivalent.
- Alle Benutzer, die Zugang zum System über ungeschützte externe Leitungen erhalten wollen, benutzen den Mechanismus „Starke Authentisierung".
- Der Zugang unter besonders sicherheitskritischen Kennungen soll über den Mechanismus „Mehraugen-Prinzip" erfolgen. ***FIA_UAU.5.2***

5.1.5.7 - Re-authenticating (FIA_UAU.6)

Die TSF müssen den Benutzer unter den Bedingungen

- Ausbleiben von Ein- bzw. Ausgaben an dem Endgerät während einer aktiven Sitzung über eine in Übereinstimmung mit der Sicherheitspolitik einstellbaren Zeit
- Änderung der Authentisierungsdaten durch den Benutzer (z.B. Wechsel des Passwortes)
- Anforderung durch eine Anwendung über eine vom System bereitgestellte Programmierschnittstelle

wieder authentisieren. ***FIA_UAU.6.1***

5.1.5.8 - Protected authentication feedback (FIA_UAU.7)

Die TSF müssen sicherstellen, dass während der Authentisierung nur Rückmeldungen, die keinerlei Rückschlüsse auf evtl. eingegebene Authentisierungsgeheimnisse erlauben, an den Benutzer bereitgestellt werden. ***FIA_UAU.7.1***

5.1.5.9 - User identification before any action (FIA_UID.2)

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. ***FIA_UID.2.1***

5.1.5.10 - User-subject binding (FIA_USB.1)

The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user. ***FIA_USB.1.1***

5.1.6 - Security management (FMT)

5.1.6.1 - Management of security functions behaviour (FMT_MOF.1)

Die TSF müssen die Fähigkeit zum

- Feststellen des Verhaltens
- Deaktivieren
- Aktivieren
- Modifizieren des Verhaltens

aller konfigurierbaren Sicherheitsfunktionen auf die autorisierten identifizierten Rollen beschränken. ***FMT_MOF.1.1***

5.1.6.2 - Management of security attributes (FMT_MSA.1)

Die TSF müssen die benutzerbestimmte Zugriffskontrolle (DAC) zur Beschränkung der Fähigkeit zum Modifizieren der Sicherheitsattribute auf die identifizierten Rollen durchsetzen. ***FMT_MSA.1.1***

5.1.6.3 - Secure security attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are accepted for security attributes. ***FMT_MSA.2.1***

5.1.6.4 - Static attribute initialisation (FMT_MSA.3)

Die TSF müssen die benutzerbestimmte Zugriffskontrolle (DAC) zur Bereitstellung von vorgegebenen Standardwerten mit einschränkenden Eigenschaften für Sicherheitsattribute, die zur Durchsetzung der SFP benutzt werden, durchsetzen. ***FMT_MSA.3.1***

Die TSF müssen dem Ersteller eines Objektes gestatten, bei der Erzeugung eines Objekts oder von Informationen alternative Anfangswerte zu spezifizieren, die die vorgegebenen Standardwerte ersetzen. ***FMT_MSA.3.2***

5.1.6.5 - Management of TSF data (FMT_MTD.1)
Die TSF müssen die Fähigkeit zum
• Standardvorgaben ändern,
• Abfragen,
• Modifizieren,
• Löschen,
• Zurücksetzen,
• [Zuweisung: andere Operationen] (z.B. Erzeugen) folgender TSF-Daten auf folgende Rollen beschränken:
TSF-Daten --- Rollen
Protokollierungsdaten des Audit-Trails --- Auditor
System-Konfigurationsdateien --- Sicherheits-Systemtechniker
Audit-Konfigurationsdateien (z.B.Liste der zu protokollierenden Ereignisse) --- Auditor
Benutzerkonten-Datenbanken (z.B. Authentisierungsdaten) --- Sicherheitsadministrator für die Benutzerverwaltung
Systemuhr --- Systemadministrator
[Zuweisung: Liste weiterer TSFDaten] ---[Zuweisung: autorisierten identifizierten Rollen]
FMT_MTD.1.1

5.1.6.6 - Management of limits on TSF data (FMT_MTD.2)
Die TSF müssen die Spezifikation der Begrenzungen für
• die Größe des Audit-Trails
auf die Rolle des Auditors beschränken. ***FMT_MTD.2.1***

Die TSF müssen die folgenden Aktionen ausführen, wenn TSF-Daten die angezeigten Begrenzungen erreicht haben oder diese überschreiten:
• Das System soll einen Alarm auslösen und einem verantwortlichen Systemadministrator zustellen, wenn die Größe des Audit-Trails eine vorbestimmte Grenze überschreitet. ***FMT_MTD.2.2***

5.1.6.7 - Revocation (FMT_REV.1)
The TSF shall restrict the ability to revoke security attributes associated with the users subjects objects other additional resources within the TSC to the authorised identified roles. ***FMT_REV.1.1***

Die TSF müssen die folgenden Regeln
• Änderungen der Sicherheitsattribute eines Objektes werden spätestens beim nächsten Öffnen des Objektes wirksam.
• Änderungen der Sicherheitsattribute eines Benutzers werden spätestens beim nächsten Anmeldeversuch des Benutzers wirksam.
• Änderungen der globalen Sicherheitsattribute eines Systems werden spätestens beim nächsten erfolgreichen Neustart des Systems wirksam.
• In verteilten Systemen ist der Widerruf zeitnah, d.h. zum nächstmöglichen Zeitpunkt, durchzuführen.
durchsetzen. ***FMT_REV.1.2***

5.1.6.8 - Time-limited authorisation (FMT_SAE.1)

TSF müssen die Berechtigung zur Spezifikation einer Verfallzeit für
- Benutzerkennungen
- Benutzerwählbare Authentisierungsgeheimnisse (Passwörter)
- Tickets bzw. Credentials zur Authentisierung eines Benutzers oder Dienstes

auf die Rollen des Sicherheits-Systemtechnikers, des Sicherheitsadministrators für die Benutzerverwaltung und des Systemadministrators beschränken. ***FMT_SAE.1.1***

Für jedes dieser Sicherheitsattribute müssen die TSF in der Lage sein, nach Ablauf der Verfallzeit für die angezeigten Sicherheitsattribute die folgenden Aktionen auszuführen.
- Nach Ablauf der Gültigkeit einer Benutzerkennung darf das System keine Anmeldung des Benutzers mehr erlauben, d.h. jede Identifizierung und Authentisierung des Benutzers muss fehlschlagen.
- Das System muss beim Ablauf eines Authentisierungsgeheimnisses den Benutzer zur Änderung seines Authentisierungsgeheimnisses zwingen. Voraussetzung für die Änderung des Authentisierungsgeheimnisses ist die erfolgreiche Authentisierung des Benutzers mit dem alten Authentisierungsgeheimnis.
- Das System muss einen geschützten Mechanismus zur Verfügung stellen, der Benutzer beim Ablauf ihres Authentisierungsgeheimnisses warnt. Die Warnung der Benutzer vor dem Ablauf ihres Authentisierungsgeheimnisses kann geschehen entweder
- durch Benachrichtigung des betroffenen Benutzers während eines spezifizierbaren Zeitraums vor dem Ablauf der Gültigkeit des Authentisierungsgeheimnisses oder
- durch Benachrichtigung des betroffenen Benutzers bei Ablauf der Gültigkeit des Authentisierungsgeheimnisses und Zulassen einer spezifizierbaren Anzahl zusätzlicher Anmeldungen, bevor die Kennung dieses Benutzers gesperrt wird.
- Beim Ablauf eines Tickets darf das System keine Autorisierungen, die unter Vorlage dieses Tickets angefordert werden, mehr gewähren.

FMT_SAE.1.2

5.1.6.9 - Security roles (FMT_SMR.1)

Die TSF müssen die folgenden Rollen
- Systemadministrator
- Sicherheitsadministrator für die Rollenverwaltung
- Sicherheitsadministrator für die Benutzerverwaltung
- Auditor
- Kryptobeauftragter
- Sicherheits-Systemtechniker
- Revisor
- Operator
- Einfacher Benutzer

erhalten. ***FMT_SMR.1.1***

The TSF shall be able to associate users with roles. ***FMT_SMR.1.2***

5.1.6.10 - Restrictions on security roles (FMT_SMR.2)
Die TSF müssen die folgenden Rollen
• Systemadministrator
• Sicherheitsadministrator für die Rollenverwaltung
• Sicherheitsadministrator für die Benutzerverwaltung
• Auditor
• Kryptobeauftragter
• Sicherheits-Systemtechniker
• Revisor
• Operator
• Einfacher Benutzer
erhalten. ***FMT_SMR.2.1***

The TSF shall be able to associate users with roles. ***FMT_SMR.2.2***

Die TSF müssen sicherstellen, dass die folgenden Bedingungen
• Wenn ein Benutzer die Revisorrolle innehat, darf er gleichzeitig keine andere Rolle einnehmen.
• Wenn das System es erlaubt, ist die Rolle des Auditors von allen anderen administrativen Rollen zu trennen und die Einnahme einer administrativen Rolle darf nicht gleichzeitig mit der Einnahme der Rolle des Auditors geschehen.
erfüllt werden. ***FMT_SMR.2.3***

5.1.6.11 - Assuming roles (FMT_SMR.3)
Die TSF müssen eine explizite Anforderung zur Annahme der folgenden Rollen erfordern:
• Systemadministrator
• Sicherheitsadministrator für die Rollenverwaltung
• Sicherheitsadministrator für die Benutzerverwaltung
• Auditor
• Kryptobeauftragter
• Sicherheits-Systemtechniker
• Operator
• Revisor
FMT_SMR.3.1

5.1.7 - Protection of the TOE Security Functions (FPT)

5.1.7.1 - Abstract machine testing (FPT_AMT.1)
The TSF shall run a suite of tests during initial start-up at the request of an authorised user other conditions to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. ***FPT_AMT.1.1***

5.1.7.2 - Failure with preservation of secure state (FPT_FLS.1)
Die TSF müssen den sicheren Zustand bei Auftreten folgender Fehlerarten:
- alle Fehlerarten einschließlich schwerwiegender Ausnahmefehler erhalten. ***FPT_FLS.1.1***

5.1.7.3 - Inter-TSF availability within a defined availability metric (FPT_ITA.1)
Die TSF müssen die Verfügbarkeit von allen für sicherheitsrelevante Entscheidungen benötigten Daten, die für ein entferntes vertrauenswürdiges IT-Produkt bereitgestellt sind, innerhalb [Zuweisung: definierte Verfügbarkeitsmetrik] unter folgenden Bedingungen [Zuweisung: Bedingungen zum Sicherstellen der Verfügbarkeit] sicherstellen. ***FPT_ITA.1.1***

5.1.7.4 - Inter-TSF confidentiality during transmission (FPT_ITC.1)
The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission. **FPT_ITC.1.1**

5.1.7.5 - Inter-TSF detection of modification (FPT_ITI.1)
Die TSF müssen die Fähigkeit bereitstellen, jede Modifizierung von TSFDaten während der Übertragung zwischen den TSF und einem entfernten vertrauenswürdigen IT-Produkt innerhalb der folgenden Metrik: [Zuweisung: eine definierte Modifizierungsmetrik] zu erkennen. ***FPT_ITI.1.1***

Die TSF müssen die Fähigkeit bereitstellen, die Integrität aller zwischen den TSF und einem entfernten, vertrauenswürdigen IT-Produkt übertragenen TSF-Daten zu verifizieren, und, falls Modifizierungen erkannt werden [Zuweisung: auszuführende Aktion] ausführen. ***FPT_ITI.1.2***

5.1.7.6 - Resistance to physical attack (FPT_PHP.3)
The TSF shall resist physical tampering scenarios to the list of TSF devices/elements by responding automatically such that the TSP is not violated. ***FPT_PHP.3.1***

5.1.7.7 - Manual recovery (FPT_RCV.1)
After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. ***FPT_RCV.1.1***

5.1.7.8 - Replay detection (FPT_RPL.1)
TSF müssen eine Wiedereinspielung für die folgenden Einheiten erkennen:
- Authentisierungsdaten
- Tickets / Credentials.
- alle Daten einer geschützten Verbindung

FPT_RPL.1.1

Die TSF müssen bei Erkennung von Wiedereinspielung
- eine Zurückweisung der Aktion, die mit den wieder eingespielten Daten in Verbindung steht und
- eine Protokollierung des Vorfalls

durchführen. ***FPT_RPL.1.2***

5.1.7.9 - Non-bypassability of the TSP (FPT_RVM.1)
The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. ***FPT_RVM.1.1***

5.1.7.10 - SFP domain separation (FPT_SEP.2)
The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. ***FPT_SEP.2.1***

The TSF shall enforce separation between the security domains of subjects in the TSC. ***FPT_SEP.2.2***

Die TSF müssen den Teil der TSF, der zu der benutzerbestimmten Zugriffskontrolle in Beziehung steht, in einem Sicherheitsbereich für deren eigene Ausführung aufrechterhalten, der diese vor Eingriffen und Manipulationen durch den Rest der TSF und durch in Bezug auf diese SFPs nichtvertrauenswürdige Subjekte schützt. ***FPT_SEP.2.3***

5.1.7.11 - Reliable time stamps (FPT_STM.1)
The TSF shall be able to provide reliable time stamps for its own use. ***FPT_STM.1.1***

5.1.7.12 - TSF testing (FPT_TST.1)
The TSF shall run a suite of self tests during initial start-up at the request of the authorised user to demonstrate the correct operation of the TSF. ***FPT_TST.1.1***

The TSF shall provide authorised users with the capability to verify the integrity of TSF data. ***FPT_TST.1.2***

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. ***FPT_TST.1.3***

5.1.8 - TOE access (FTA)

5.1.8.1 - Limitation on scope of selectable attributes (FTA_LSA.1)

Comment [i5]: fraglich?

Die TSF müssen den Anwendungsbereich der Sitzungs-Sicherheitsattribute „Auswahl einer Rolle" basierend auf
- dem Zeitpunkt des Zuganges,
- dem Ort des Zuganges,
- der Art des Zuganges,
- einer Liste anderer ausgewählter Rollen

einschränken. ***FTA_LSA.1.1***

5.1.8.2 - Basic limitation on multiple concurrent sessions (FTA_MCS.1)

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user. ***FTA_MCS.1.1***
Die TSF müssen als Standardvorgabe eine Begrenzung auf maximal eine Sitzung pro Benutzer durchsetzen. ***FTA_MCS.1.2***

5.1.8.3 - TSF-initiated session locking (FTA_SSL.1)

Die TSF müssen eine interaktive Sitzung nach Ablauf einer in Übereinstimmung mit der Sicherheitspolitik einstellbaren Zeitspanne ohne Benutzeraktivität sperren, und zwar durch:
- Löschen oder Überschreiben von Anzeigegeräten, wobei die gegenwärtigen Inhalte unlesbar gemacht werden
- Deaktivierung aller Aktivitäten von Zugriffs-/Anzeigegeräten außer dem Entsperren der Sitzung. ***FTA_SSL.1.1***

Die TSF müssen das Eintreten folgender Ereignisse vor dem Entsperren der Sitzung erfordern:
- Der dieser Sitzung zugeordnete Benutzer muss vom System erneut authentisiert worden sein. ***FTA_SSL.1.2***

5.1.8.4 - User-initiated locking (FTA_SSL.2)

The TSF shall allow user-initiated locking of the user's own interactive session, by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session. ***FTA_SSL.2.1***

Die TSF müssen das Eintreten folgender Ereignisse vor dem Entsperren der Sitzung erfordern:

• Der dieser Sitzung zugeordnete Benutzer muss vom System erneut authentisiert worden sein. ***FTA_SSL.2.2***

5.1.8.5 - TOE access history (FTA_TAH.1)

Upon successful session establishment, the TSF shall display the date time location of the last successful session establishment to the user. ***FTA_TAH.1.1***

Upon successful session establishment, the TSF shall display the date time location of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment. ***FTA_TAH.1.2***

The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information. ***FTA_TAH.1.3***

5.1.8.6 - TOE session establishment (FTA_TSE.1)

Comment [i6]: fraglich?

Die TSF müssen in der Lage sein, basierend auf
• dem Zeitpunkt der Anforderung einer Sitzungseinrichtung,
• dem Zugangspunkt, von dem aus eine Sitzungseinrichtung angefordert wird,
• der Benutzerkennung, für die eine Sitzungseinrichtung angefordert wird
eine Sitzungseinrichtung zu verweigern. ***FTA_TSE.1.1***

5.1.9 - Trusted path/channels (FTP)

5.1.9.1 - Inter-TSF trusted channel (FTP_ITC.1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. ***FTP_ITC.1.1***

The TSF shall permit the TSF to initiate communication via the trusted channel. ***FTP_ITC.1.2***

Die TSF müssen für
• die Übertragung sämtlicher sicherheitsrelevanter Systemdaten
• die Übertragung sämtlicher sicherheitsrelevanter Benutzerdaten
eine Kommunikation über den vertrauenswürdigen Kanal einleiten. ***FTP_ITC.1.3***

5.1.9.2 - Trusted path (FTP_TRP.1)

The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides

assured identification of its end points and protection of the communicated data from modification or disclosure. ***FTP_TRP.1.1***

The TSF shall permit the TSF to initiate communication via the trusted path. ***FTP_TRP.1.2***

Die TSF müssen den Gebrauch des vertrauenswürdigen Pfads für
• die Erst-Benutzerauthentisierung,
• die Benutzung des Authentisierungsmechanismus (z.B. zur Re-Authentisierung),
• die Eingabe von sensitiven Informationen
erfordern. ***FTP_TRP.1.3***

5.2 - TOE Security Assurance Requirements

Table 5-1 Assurance Requirements: EAL(2)

Assurance Class	Assurance Components
ACM	ACM_CAP.2
ADO	ADO_DEL.1 ADO_IGS.1
ADV	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1
AGD	AGD_ADM.1 AGD_USR.1
ATE	ATE_COV.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_SOF.1 AVA_VLA.1

5.2.1 - Configuration management (ACM)

5.2.1.1 - Configuration items (ACM_CAP.2)

The reference for the TOE shall be unique to each version of the TOE. ***ACM_CAP.2.1C***

The developer shall provide a reference for the TOE. ***ACM_CAP.2.1D***

The TOE shall be labelled with its reference. ***ACM_CAP.2.2C***

The developer shall use a CM system. ***ACM_CAP.2.2D***

The CM documentation shall include a configuration list. ***ACM_CAP.2.3C***

The developer shall provide CM documentation. ***ACM_CAP.2.3D***

The configuration list shall describe the configuration items that comprise the TOE. ***ACM_CAP.2.4C***

The CM documentation shall describe the method used to uniquely identify the configuration items. ***ACM_CAP.2.5C***

The CM system shall uniquely identify all configuration items. ***ACM_CAP.2.6C***

5.2.2 - Delivery and operation (ADO)

5.2.2.1 - Delivery procedures (ADO_DEL.1)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site. ***ADO_DEL.1.1C***

The developer shall document procedures for delivery of the TOE or parts of it to the user. ***ADO_DEL.1.1D***

The developer shall use the delivery procedures. ***ADO_DEL.1.2D***

5.2.2.2 - Installation, generation, and start-up procedures (ADO_IGS.1)

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. ***ADO_IGS.1.1C***

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE. ***ADO_IGS.1.1D***

5.2.3 - Development (ADV)

5.2.3.1 - Informal functional specification (ADV_FSP.1)

The functional specification shall describe the TSF and its external interfaces using an informal style. ***ADV_FSP.1.1C***

The developer shall provide a functional specification. ***ADV_FSP.1.1D***

The functional specification shall be internally consistent. ***ADV_FSP.1.2C***

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate. ***ADV_FSP.1.3C***

The functional specification shall completely represent the TSF. ***ADV_FSP.1.4C***

5.2.3.2 - Descriptive high-level design (ADV_HLD.1)

The presentation of the high-level design shall be informal. ***ADV_HLD.1.1C***

The developer shall provide the high-level design of the TSF. ***ADV_HLD.1.1D***

The high-level design shall be internally consistent. ***ADV_HLD.1.2C***

The high-level design shall describe the structure of the TSF in terms of subsystems. ***ADV_HLD.1.3C***

The high-level design shall describe the security functionality provided by each subsystem of the TSF. ***ADV_HLD.1.4C***

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software. ***ADV_HLD.1.5C***

The high-level design shall identify all interfaces to the subsystems of the TSF. ***ADV_HLD.1.6C***

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible. ***ADV_HLD.1.7C***

5.2.3.3 - Informal correspondence demonstration (ADV_RCR.1)

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. ***ADV_RCR.1.1C***

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided. ***ADV_RCR.1.1D***

5.2.4 - Guidance documents (AGD)

5.2.4.1 - Administrator guidance (AGD_ADM.1)

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE. ***AGD_ADM.1.1C***

The developer shall provide administrator guidance addressed to system administrative personnel. ***AGD_ADM.1.1D***

The administrator guidance shall describe how to administer the TOE in a secure manner. ***AGD_ADM.1.2C***

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment. ***AGD_ADM.1.3C***

The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE. ***AGD_ADM.1.4C***

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate. ***AGD_ADM.1.5C***

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. ***AGD_ADM.1.6C***

The administrator guidance shall be consistent with all other documentation supplied for evaluation. ***AGD_ADM.1.7C***

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator. ***AGD_ADM.1.8C***

5.2.4.2 - User guidance (AGD_USR.1)

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. ***AGD_USR.1.1C***

The developer shall provide user guidance. ***AGD_USR.1.1D***

The user guidance shall describe the use of user-accessible security functions provided by the TOE. ***AGD_USR.1.2C***

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. ***AGD_USR.1.3C***

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment. ***AGD_USR.1.4C***

The user guidance shall be consistent with all other documentation supplied for evaluation. ***AGD_USR.1.5C***

The user guidance shall describe all security requirements for the IT environment that are relevant to the user. ***AGD_USR.1.6C***

5.2.5 - Tests (ATE)

5.2.5.1 - Evidence of coverage (ATE_COV.1)

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. ***ATE_COV.1.1C***

The developer shall provide evidence of the test coverage. ***ATE_COV.1.1D***

5.2.5.2 - Functional testing (ATE_FUN.1)

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results. ***ATE_FUN.1.1C***

The developer shall test the TSF and document the results. ***ATE_FUN.1.1D***

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed. ***ATE_FUN.1.2C***

The developer shall provide test documentation. ***ATE_FUN.1.2D***

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests. ***ATE_FUN.1.3C***

The expected test results shall show the anticipated outputs from a successful execution of the tests. ***ATE_FUN.1.4C***

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified. ***ATE_FUN.1.5C***

5.2.5.3 - Independent testing - sample (ATE_IND.2)

The TOE shall be suitable for testing. ***ATE_IND.2.1C***

The developer shall provide the TOE for testing. ***ATE_IND.2.1D***

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. ***ATE_IND.2.2C***

5.2.6 - Vulnerability assessment (AVA)

5.2.6.1 - Strength of TOE security function evaluation (AVA_SOF.1)

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST. ***AVA_SOF.1.1C***

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim. ***AVA_SOF.1.1D***

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST. ***AVA_SOF.1.2C***

5.2.6.2 - Developer vulnerability analysis (AVA_VLA.1)

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. ***AVA_VLA.1.1C***

The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP. ***AVA_VLA.1.1D***

The developer shall document the disposition of obvious vulnerabilities. ***AVA_VLA.1.2D***

5.3 - Security Requirements for the IT Environment (Optional)

Derzeit keine Anforderungen.

5.4 - Security Requirements for the Non-IT Environment (Optional)

Derzeit keine Anforderungen.

6 - Rationale

Auf die Ausführung von Erklärungen wurde verzichtet.

6.1 - Introduction and TOE Description Rationale (Optional)

Derzeit keine Erklärungen vorhanden.

6.2 - Security Objectives Rationale

Table 6-1 Mapping Threats to Security Objectives

Bedrohung	**Entgegenwirkendes Sicherheitsziel**
Vom EVG abzuwehrende Bedrohungen	
B.Zugang	Z.Zugang, Z.Partner, Z.Verbindung, Z.KommAdmin, Z.Zeit-Ort, Z.Benutzer, Z.Geheim, Z.Admin, Z.SysAdmin, Z.Verantwortung, Z.Zugriff, Z.Software, Z.Betrieb, Z.Installation, Z.Fehler, Z.Umgehung, Z.Zutritt, Z.Schutz
B.Zugriff	Z.Zugriff, Z.Zugang, Z.Benutzer, Z.Admin, Z.SysAdmin, Z.Verantwortung, Z.Status, Z.Definition Z.Installation, Z.Software, Z.Fehler, Z.Betrieb, Z.Verbindung, Z.Partner, Z.KommAdmin, Z.Umgehung, Z.Zutritt, Z.Schutz
B.Fehler	Z.Fehler, Z.Software, Z.Betrieb, Z.Zustand, Z.Status, Z.Archiv
B.Absturz	Z.Zustand, Z.Archiv, Z.Software, Z.Betrieb
B.Verfügbarkeit	Z.Verfügbarkeit, Z.SysAdmin, Z.KommAdmin, Z.Zugang, Z.Zugriff, Z.Verantwortung, Z.Benutzer, Z.Zustand, Z.Archiv, Z.Software, Z.Betrieb, Z.Aufbewahrung
B.Beweis	Z.Verantwortung, Z.SysAdmin, Z.Archiv,

	Z.Aufbewahrung, Z.Umgehung, Z.Zugang, Z.Zugriff, Z.Verbindung, Z.Fehler, Z.Software, Z.Betrieb, Z.Zustand
B.Manipulation	Z.Zugriff, Z.Verbindung, Z.Fehler, Z.Umgehung, Z.Software, Z.Betrieb, Z.Zustand, Z.Admin, Z.SysAdmin, Z.Installation, Z.Status, Z.Schutz, Z.Zutritt
B.Erkennen	Z.Status, Z.Verfügbarkeit, Z.Betrieb, Z.Admin, Z.SysAdmin, Z.Fehler, Z.Software
Von der Betriebsumgebung abzuwehrende Bedrohungen	
B.Installation	Z.Installation, Z.Status, Z.Admin, Z.SysAdmin
B.Gewalt	Z.Schutz, Z.Zutritt, Z.Admin, Z.Status, Z.SysAdmin
B.Rollen	Z.Definition, Z.Admin, Z.SysAdmin

Table 6-2 Mapping of Security Objectives to SecurityFunctions

Sicherheitsziel	**Sicherheitsanforderung**
Sicherheitsziele für den EVG	
Z.Zugang	FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_UID.2, FMT_MSA.3, FMT_REV.1, FMT_SAE.1, FPT_PHP.3, FPT_RPL.1, FTA_MCS.1, FTA_SSL.1, FTA_SSL.2, FTA_TSE.1, FTP_TRP.1
Z.Zugriff	FAU_SAR.2, FAU_STG.2, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FDP_RIP.2, FDP_UCT.1, FDP_UIT.1, FIA_ATD.1, FIA_UAU.6, FIA_UID.2, FIA_USB.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1,FMT_MTD.2, FMT_REV.1, FMT_SMR.1, FMT_SMR.2,

	FPT_PHP.3, FPT_RPL.1, FTA_MCS.1, FTA_SSL.1, FTA_SSL.2
Z.Archiv	FDP_SDI.2, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_RCV.1, FDP_UCT.1, FDP_UIT.1
Z.Verantwortung	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.2, FAU_STG.4, FCO_NRO.1, FCO_NRR.1, FDP_ACC.1, FDP_ACF.1, FIA_SOS.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_UID.2, FIA_USB.1, FMT_MTD.1, FMT_MTD.2, FMT_SMR.3, FPT_RPL.1, FPT_STM.1, FTA_MCS.1, FTA_TAH.1
Z.Zeit-Ort	FIA_ATD.1, FMT_SAE.1, FPT_STM.1, FTA_LSA.1, FTA_TSE.1
Z.Schutz	FPT_PHP.3
Z.Umgehung	EAL4, FAU_STG.2, FAU_STG.4, FIA_AFL.1, FIA_UAU.4, FPT_ITI.1, FPT_PHP.3, FPT_RPL.1, FPT_RVM.1, FPT_SEP.2, FTP_ITC.1, FTP_TRP.1, FTP_ITC.1
Z.Fehler	ADV_INT.1, ALC_FLR.3, EAL4, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.5, FMT_MSA.2, FMT_SAE.1, FPT_ITC.1, FTA_SSL.1
Z.SysAdmin	EAL4, FAU_SEL.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1, FMT_SAE.1, FMT_SMR.1, FMT_SMR.2, FMT_SMR.3
Z.Betrieb	ADV_INT.1, ALC_FLR.3, EAL4, FDP_SDI.2, FIA_UAU.5, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.2, FPT_PHP.3, FPT_AMT.1, FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1,

	FPT_RCV.1, FPT_RVM.1, FPT_SEP.2, FPT_TST.1
Z.Status	FAU_ARP.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FMT_MTD.1, FMT_MTD.2, FPT_AMT.1, FPT_TST.1, FTA_TAH.1
Z.Verbindung	FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FIA_AFL.1, FIA_UAU.4, FIA_UAU.5, FMT_SAE.1, FPT_ITA.1, FPT_ITI.1, FPT_ITC.1, FPT_RPL.1, FPT_RVM.1, FPT_SEP.2, FTP_ITC.1, FTP_TRP.1
Z.Verfügbarkeit	FPT_ITA.1
Z.Zustand	EAL4, FAU_STG.4, FDP_SDI.2, FPT_AMT.1, FPT_FLS.1, FPT_PHP.3, FPT_TST.1
Z.Software	ADV_INT.1, ALC_FLR.3, EAL4
Sicherheitsziele für die Umgebung	
Z.Installation	FPT_AMT.1, FPT_TST.1
Z.Definition	FDP_ACC.1, FDP_ACF.1, FTA_LSA.1
Z.Geheim	FIA_UAU.7

6.2.1 - Policies

Derzeit keine Erklärungen vorhanden.

6.2.2 - Threats

Derzeit keine Erklärungen vorhanden.

6.3 - Security Requirements Rationale

Derzeit keine Erklärungen vorhanden.

6.3.1 - Functional Security Requirements Rationale

Table 6-3 Functional Component to Security Objective Mapping

Objectives	Requirements
Security Objectives	ACM_CAP.2, ADO_DEL.1, ADO_IGS.1, ADV_FSP.1, ADV_HLD.1, ADV_RCR.1, AGD_ADM.1, AGD_USR.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2, AVA_SOF.1, AVA_VLA.1, FIA_UID.2, FIA_USB.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_SOS.1, FIA_AFL.1, FTA_TSE.1, FTA_LSA.1, FTA_SSL.1, FTA_SSL.2, FTA_MCS.1, FTA_TAH.1, FDP_ACC.1, FDP_ACF.1, FDP_SDI.2, FDP_UCT.1, FDP_UIT.1, FDP_RIP.2, FPT_PHP.3, FPT_RVM.1, FPT_SEP.2, FPT_AMT.1, FPT_TST.1, FPT_FLS.1, FPT_RCV.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_RPL.1, FPT_STM.1, FCO_NRO.1, FCO_NRR.1, FTP_TRP.1, FTP_ITC.1, FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FAU_GEN.1, FAU_GEN.2, FAU_SEL.1, FAU_SAA.1, FAU_ARP.1, FAU_STG.2, FAU_STG.4, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1, FMT_SAE.1, FMT_SMR.1, FMT_SMR.2, FMT_SMR.3

Security Objectives:

Security Objectives is implemented in the TOE by:

ACM_CAP.2: Configuration items
ADO_DEL.1: Delivery procedures
ADO_IGS.1: Installation, generation, and start-up procedures
ADV_FSP.1: Informal functional specification
ADV_HLD.1: Descriptive high-level design
ADV_RCR.1: Informal correspondence demonstration
AGD_ADM.1: Administrator guidance
AGD_USR.1: User guidance
ATE_COV.1: Evidence of coverage
ATE_FUN.1: Functional testing
ATE_IND.2: Independent testing - sample
AVA_SOF.1: Strength of TOE security function evaluation
AVA_VLA.1: Developer vulnerability analysis
FIA_UID.2: User identification before any action
FIA_USB.1: User-subject binding
FIA_ATD.1: User attribute definition
FIA_UAU.2: User authentication before any action
FIA_UAU.4: Single-use authentication mechanisms
FIA_UAU.5: Multiple authentication mechanisms
FIA_UAU.6: Re-authenticating
FIA_UAU.7: Protected authentication feedback
FIA_SOS.1: Verification of secrets
FIA_AFL.1: Authentication failure handling

FTA_TSE.1:	TOE session establishment
FTA_LSA.1:	Limitation on scope of selectable attributes
FTA_SSL.1:	TSF-initiated session locking
FTA_SSL.2:	User-initiated locking
FTA_MCS.1:	Basic limitation on multiple concurrent sessions
FTA_TAH.1:	TOE access history
FDP_ACC.1:	Subset access control
FDP_ACF.1:	Security attribute based access control
FDP_SDI.2:	Stored data integrity monitoring and action
FDP_UCT.1:	Basic data exchange confidentiality
FDP_UIT.1:	Data exchange integrity
FDP_RIP.2:	Full residual information protection
FPT_PHP.3:	Resistance to physical attack
FPT_RVM.1:	Non-bypassability of the TSP
FPT_SEP.2:	SFP domain separation
FPT_AMT.1:	Abstract machine testing
FPT_TST.1:	TSF testing
FPT_FLS.1:	Failure with preservation of secure state
FPT_RCV.1:	Manual recovery
FPT_ITA.1:	Inter-TSF availability within a defined availability metric
FPT_ITC.1:	Inter-TSF confidentiality during transmission
FPT_ITI.1:	Inter-TSF detection of modification
FPT_RPL.1:	Replay detection
FPT_STM.1:	Reliable time stamps
FCO_NRO.1:	Selective proof of origin
FCO_NRR.1:	Selective proof of receipt
FTP_TRP.1:	Trusted path
FTP_ITC.1:	Inter-TSF trusted channel
FCS_COP.1:	Cryptographic operation
FCS_CKM.1:	Cryptographic key generation
FCS_CKM.2:	Cryptographic key distribution
FCS_CKM.3:	Cryptographic key access
FCS_CKM.4:	Cryptographic key destruction
FAU_GEN.1:	Audit data generation
FAU_GEN.2:	User identity association
FAU_SEL.1:	Selective audit
FAU_SAA.1:	Potential violation analysis
FAU_ARP.1:	Security alarms
FAU_STG.2:	Guarantees of audit data availability
FAU_STG.4:	Prevention of audit data loss
FAU_SAR.1:	Audit review
FAU_SAR.2:	Restricted audit review
FAU_SAR.3:	Selectable audit review
FMT_MOF.1:	Management of security functions behaviour
FMT_MSA.1:	Management of security attributes
FMT_MSA.2:	Secure security attributes
FMT_MSA.3:	Static attribute initialisation
FMT_MTD.1:	Management of TSF data

FMT_MTD.2: Management of limits on TSF data
FMT_REV.1: Revocation
FMT_SAE.1: Time-limited authorisation
FMT_SMR.1: Security roles
FMT_SMR.2: Restrictions on security roles
FMT_SMR.3: Assuming roles

6.3.2 - Assurance Security Requirements Rationale

Derzeit keine Erklärungen vorhanden.

6.4 - Dependency Rationale

Table 6-4 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FAU_ARP.1	FAU_SAA.1
FAU_GEN.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1
FAU_SAA.1	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.2	FAU_GEN.1
FAU_STG.4	FAU_STG.1
FCO_NRO.1	FIA_UID.1
FCO_NRR.1	FIA_UID.1
FCS_CKM.1	FCS_CKM.2, FCS_COP.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.3	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FDP_UCT.1	FTP_ITC.1, FTP_TRP.1, FDP_ACC.1,
FDP_UIT.1	FDP_ACC.1, FTP_ITC.1, FTP_TRP.1

FIA_AFL.1	FIA_UAU.1
FIA_UAU.2	FIA_UID.1
FIA_UAU.7	FIA_UAU.1
FIA_USB.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.2	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1
FMT_REV.1	FMT_SMR.1
FMT_SAE.1	FMT_SMR.1, FPT_STM.1
FMT_SMR.1	FIA_UID.1
FMT_SMR.2	FIA_UID.1
FMT_SMR.3	FMT_SMR.1
FPT_FLS.1	-
FPT_RCV.1	FPT_TST.1, AGD_ADM.1,
FPT_TST.1	FPT_AMT.1
FTA_MCS.1	FIA_UID.1
FTA_SSL.1	FIA_UAU.1
FTA_SSL.2	FIA_UAU.1
Assurance Requirements	
ADO_IGS.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1, ADV_RCR.1
AGD_ADM.1	ADV_FSP.1

AGD_USR.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1, ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

Justification of Unsupported Dependencies

6.5 - Security Functional Requirements Grounding in Objectives

Table 6-5 Function to Objectives Mapping

Function	Objectives
FAU_ARP.1	Z.Status, Z.Verantwortung
FAU_GEN.1	Z.Verantwortung
FAU_GEN.2	Z.Verantwortung
FAU_SAA.1	Z.Status, Z.Verantwortung
FAU_SAR.1	Z.Status, Z.Verantwortung
FAU_SAR.2	Z.Zugriff
FAU_SAR.3	Z.Status, Z.Verantwortung
FAU_SEL.1	Z.SysAdmin, Z.Verantwortung
FAU_STG.2	Z.Umgehung, Z.Verantwortung, Z.Zugriff
FAU_STG.4	Z.Umgehung, Z.Verantwortung, Z.Zustand
FCO_NRO.1	Z.Verantwortung
FCO_NRR.1	Z.Verantwortung
FCS_CKM.1	Z.Fehler, Z.SysAdmin, Z.Zugriff
FCS_CKM.2	Z.Fehler, Z.SysAdmin, Z.Zugriff
FCS_CKM.3	Z.Fehler, Z.SysAdmin, Z.Verbindung, Z.Zugriff
FCS_CKM.4	Z.Fehler, Z.SysAdmin, Z.Verbindung, Z.Zugriff
FCS_COP.1	Z.Fehler, Z.Verbindung, Z.Zugriff
FDP_ACC.1	Z.Verantwortung, Z.Zugriff, Z.Definition
FDP_ACF.1	Z.Verantwortung, Z.Zugriff, Z.Verbindung, Z.Definition
FDP_RIP.2	Z.Zugriff
FDP_SDI.2	Z.Betrieb, Z.Zustand, Z.Archiv
FDP_UCT.1	Z.Zugriff, Z.Verbindung, Z.Archiv
FDP_UIT.1	Z.Verbindung, Z.Zugriff, Z.Archiv

FIA_AFL.1	Z.Fehler, Z.Umgehung, Z.Verbindung, Z.Zugang
FIA_ATD.1	Z.Zeit-Ort, Z.Zugang, Z.Zugriff
FIA_SOS.1	Z.Fehler, Z.Verantwortung, Z.Zugang
FIA_UAU.2	Z.Zugang
FIA_UAU.4	Z.Umgehung, Z.Verantwortung, Z.Verbindung, Z.Zugang
FIA_UAU.5	Z.Betrieb, Z.Fehler, Z.Verantwortung, Z.Verbindung, Z.Zugang
FIA_UAU.6	Z.Verantwortung, Z.Zugang, Z.Zugriff
FIA_UAU.7	Z.Geheim, Z.Verantwortung, Z.Zugang
FIA_UID.2	Z.Verantwortung, Z.Zugang, Z.Zugriff
FIA_USB.1	Z.Verantwortung, Z.Zugriff
FMT_MOF.1	Z.Betrieb, Z.SysAdmin, Z.Zugriff
FMT_MSA.1	Z.Betrieb, Z.SysAdmin, Z.Zugriff
FMT_MSA.2	Z.Betrieb, Z.Fehler, Z.SysAdmin
FMT_MSA.3	Z.Betrieb, Z.SysAdmin, Z.Zugang, Z.Zugriff
FMT_MTD.1	Z.Status, Z.SysAdmin, Z.Verantwortung., Z.Zugriff
FMT_MTD.2	Z.Betrieb, Z.Status, Z.SysAdmin, Z.Verantwortung, Z.Zugriff
FMT_REV.1	Z.SysAdmin, Z.Zugang, Z.Zugriff
FMT_SAE.1	Z.Fehler, Z.SysAdmin, Z.Verbindung, Z.Zeit-Ort, Z.Zugang
FMT_SMR.1	Z.SysAdmin, Z.Zugriff
FMT_SMR.2	Z.SysAdmin, Z.Zugriff
FMT_SMR.3	Z.SysAdmin, Z.Verantwortung
FPT_AMT.1	Z.Betrieb, Z.Installation, Z.Status, Z.Zustand
FPT_FLS.1	Z.Betrieb, Z.Zustand
FPT_ITA.1	Z.Betrieb, Z.Verbindung, Z.Verfügbarkeit, Z.Archiv
FPT_ITC.1	Z.Betrieb, Z.Fehler, Z.Umgehung, Z.Verbindung, Z.Archiv

FPT_ITI.1	Z.Betrieb, Z.Umgehung, Z.Verbindung, Z.Archiv
FPT_PHP.3	Z.Schutz, Z.Umgehung, Z.Zugang, Z.Zugriff, Z.Zustand, Z.Betrieb
FPT_RCV.1	Z.Archiv, Z.Betrieb
FPT_RPL.1	Z.Umgehung, Z.Verantwortung, Z.Verbindung, Z.Zugang, Z.Zugriff
FPT_RVM.1	Z.Betrieb, Z.Umgehung, Z.Verbindung
FPT_SEP.2	Z.Betrieb, Z.Umgehung, Z.Verbindung
FPT_STM.1	Z.Verantwortung, Z.Zeit-Ort
FPT_TST.1	Z.Betrieb, Z.Installation, Z.Status, Z.Zustand
FTA_LSA.1	Z.Definition, Z.Zeit-Ort
FTA_MCS.1	Z.Verantwortung, Z.Zugang, Z.Zugriff
FTA_SSL.1	Z.Fehler, Z.Zugang, Z.Zugriff
FTA_SSL.2	Z.Zugang, Z.Zugriff
FTA_TAH.1	Z.Verantwortung, Z.Status
FTA_TSE.1	Z.Zugang, Z.Zeit-Ort
FTP_ITC.1	Z.Umgehung, Z.Verbindung
FTP_TRP.1	Z.Umgehung, Z.Zugang, Z.Verbindung

6.6 - Rationale for Extensions

Derzeit keine Erklärungen vorhanden.

Appendix A - Acronyms

ACL - Zugriffskontrolliste (Access Control List)
BSI - Bundesamt für Sicherheit in der Informationstechnik
CC - Common Criteria
DAC - benutzerbestimmte Zugriffskontrolle (Discretionary Access Control)
EAL - Evaluation Assurance Level
EVG - Evaluationsgegenstand (TOE – Target of Evaluation)
IT - Information Technology
PC - Arbeitsplatzrechner (Personal Computer)
PP - Protection Profile
RBAC - rollenbasierte Zugriffskontrolle (Role Based Access Control)
SF - Security Function
SFP - Security Function Policy
SOF - Strength of Function
ST - Security Target
SW - Software
TOE - Target of Evaluation
TSC - TSF Scope of Control
TSF - TOE Security Functions
TSFI - TSF Interface
TSP - TOE Security Policy

Zusammenfassung

Angriffe auf IT-Produkte sind längst keine Seltenheit mehr, wie die „Studie Hackerangriffe“ zeigt. Im Durchschnitt wurden 0,5 bis 5 ernsthafte Hackerattacken pro Monat und System ermittelt. Wenn ein Hersteller eines IT-Produkts die Gefahr von Angriffen auf sein Produkt ernst genommen und daher Gegenmaßnahmen getroffen und implementiert hat, kann er sich sein Produkt zertifizieren lassen. Eine **Sicherheitsevaluation** eines Produkts kann also den Grad des Vertrauens in ein Produkt anhand von analytischen und allgemeingültigen Kriterien belegen. Einige der größten Auftraggeber für IT-Produkte verlangen von ihren Herstellern, dass diese ihre Produkte zertifizieren lassen, um die geforderte Sicherheitsqualität einzuhalten. „In den USA werden seit Juli 2002 für den Einsatz von Produkten im Behördenbereich sowie des Militärs nur noch Produkte mit CC-Zertifikat beschafft; dies gilt sogar für Produkte, die typischerweise nicht unbedingt als IT-Sicherheitsprodukte bezeichnen werden, wie beispielsweise digitale Fotokopierer.“, so Dr. Markus Mackenbrock vom **Bundesamt für Sicherheit in der Informationstechnik**.

Nach einer Phase von nationaler Standardisierung hat sich im letzten Jahrzehnt ein internationaler Standard etabliert, auf dessen Basis heutzutage Sicherheitszertifikate allgemeingültig vergeben werden können: **Common Criteria**. Mit diesem Kriterienwerk und dem dazugehörigen Evaluationshandbuch können offiziell genehmigte Zertifizierungsstellen eine Evaluation auf Basis von Common Criteria objektiv durchführen. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Einhaltung dieses Standards verantwortlich und entscheidet, wer eine Zertifizierung auf Basis von Common Criteria durchführen darf.

Durch die **Zertifizierung** wird gewährleistet, dass ein IT-Produkt ausreichend nach folgenden Sicherheitskriterien geschützt ist:

Vertraulichkeit: Schutz vor unbefugter Kenntnisnahme von Informationen.
Integrität: Schutz vor unbefugter Veränderung von Informationen.
Verfügbarkeit: Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln.

Der offizielle Name der Common Criteria lautet „**Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik / Common Criteria for Information Technology Security Evaluation (CC)**“ [1)]. Im Mai 1998 wurde nach mehrjähriger Arbeit die Version 2.0 der Common Criteria fertig gestellt und im April 1999 die Version 2.1 veröffentlicht. Kurz darauf wurde sie von der Internationalen Standardisierungsorganisation (ISO) technisch unverändert als **Internationaler Standard ISO/IEC 15408** veröffentlicht.

Ein wesentlicher Bestandteil von CC ist, dass **Schutzprofile / Protection Profiles (PP)** die Anforderungen an die Funktionalität und die Vertrauenswürdigkeit zusammenfassen und das Sicherheitskonzept beschreiben. Außerdem werden darin die Bedrohungen den Anforderungen gegenübergestellt. Bei der folgenden Evaluation der Schutzprofile und des EVG wird dann überprüft, „ ... ob das Schutzprofil eine vollständige und in sich geschlossene Menge von Anforderungen ist und dass ein zu diesem Schutzprofil konformer EVG eine wirksame Menge von IT-Sicherheitsgegenmaßnahmen in der Sicherheitsumgebung bereitstellt.“ [1)]

Das Evaluationsergebnis muss dann auf einer **Vertrauenswürdigkeitsstufe / Evaluation Assurance Level (EAL)** basieren und dabei eventuell um weitere Anforderungen ergänzt werden. Die Ergebnisse von CC sind daher mit anderen CC Evaluationen vergleichbar.

Im Jahre 1997 wurde die erste Fassung der **Gemeinsamen Evaluationsmethodologie/ Common Evaluation Methodology (CEM)** veröffentlicht, die man als Evaluationshandbuch für CC bezeichnen kann. Dabei beschreibt CC was evaluiert und die Methodologie wie evaluiert werden soll.

Eine **Evaluation** ist der Vorgang, IT-Sicherheitsprodukte und –konzepte durch eine sachverständige Stelle zu prüfen und zu bewerten. Normalerweise werden die Evaluationsergebnisse dann durch eine Zertifizierungsstelle bestätigt. Die Festlegung der Sicherheitsanforderungen soll nach CC in verschiedenen Darstellungsebenen getroffen werden, um je nach dem Bedarf der Abstraktionsebene den EVG zu beschreiben. Eine Darstellungsebene soll eine durchdachte und überzeugende Darlegung enthalten, die zeigt, dass eine untere Ebene der höheren entspricht. Außerdem muss die Darlegung vollständig, korrekt und in sich konsistent sein, um zusammen mit den höheren Ebenen die EVG-Korrektheit zu unterstützen. Für die Vertrauenswürdigkeit des EVG tragen Erklärungen bei, die die Übereinstimmung mit den Sicherheitszielen direkt nachweisen.

Die **CC** enthalten eine hierarchische Einteilung der Sicherheitsanforderungen in Klassen, Familien und Komponenten.

Ein **Schutzprofil / Protection Profile (PP)** besteht aus einer Menge von Sicherheitsanforderungen für Standard-Sicherheitsprobleme einer Produktgruppe. Die PP fassen die Anforderungen an die Funktionalität und an die Vertrauenswürdigkeit zusammen und mittels eines ausführlichen Beschreibungsteils werden die Bedrohungen den Anforderungen gegenübergestellt. Der Beschreibungsteil stellt damit das Sicherheitskonzept dar. „Durch die Verwendung von Schutzprofilen wird daher der Aufwand bei der Erstellung von Sicherheitsvorgaben für konkrete IT-Produkte oder Systeme erheblich reduziert.“ [17)]

Die **Sicherheitsvorgaben / Security Targets (ST)** enthalten eine Menge von Sicherheitsanforderungen, die durch Verweis auf ein PP erstellt, oder explizit dargelegt werden. Mittels der ST können konkrete EVG-Sicherheitsanforderungen dargestellt werden, die für die Erfüllung der Sicherheitsziele wirksam sind. Die ST bilden die Grundlage dafür, dass alle an einer Evaluation beteiligten Seiten hinsichtlich der von einem EVG gebotenen Sicherheit übereinstimmen.

Aus der **Evaluierung** eines PP ergeben sich Evaluationsergebnisse, die in Katalogen festgehalten werden. Erst danach, wenn ein PP geprüft und bewertet wurde, kann ein ST evaluiert werden. Als Ergebnis der Evaluation steht dann eine Aussage, die beschreibt bis zu welchem Grad man dem EVG vertrauen kann, die Anforderungen zu erfüllen. Ein entscheidender Faktor für das Verständnis der Evaluation nach CC ist, sich deutlich zu machen, dass die Sicherheitsfunktionalität vom Hersteller beschrieben und ihr Vorhandensein vom **Evaluator** geprüft wird. Es können also nur vorher spezifizierte Funktionalitäten überprüft werden.

Die Entscheidung welche **Vertrauenswürdigkeitsstufe** angepeilt werden soll, hängt also unter anderem von folgenden Faktoren ab:

- Verwendungszweck
- Funktionalität des Produkts
- Bestätigung der Produktqualität
- Rechtliche und organisatorische Vorschriften
- Kostenaspekte
- Werbeeffekte
- Art des Entwicklungsprozesses
- Verfügbaren Ressourcen beim Hersteller

EAL- Stufe	Anforderungen
EAL-0	unzulängliche Vertrauenswürdigkeit
EAL-1	funktionell getestet
EAL-2	strukturell getestet
EAL-3	methodisch getestet und überprüft
EAL-4	methodisch entwickelt, getestet und durchgesehen
EAL-5	semiformal entworfen und getestet
EAL-6	semiformal verifizierter Entwurf, getestet
EAL-7	formal verifizierter Entwurf, getestet

Das Schutzprofil ist zwar nicht unbedingt nötig, aber wenn es vorhanden ist, bildet es die Grundlage der Sicherheitsvorgaben und der Evaluation. Es reduziert außerdem den Arbeitsaufwand und damit auch die Kosten. Darüber hinaus wird mit dem Schutzprofil eine Vergleichsgrundlage für alle Produkte, die nach demselben Schutzprofil bewertet werden, geschaffen. Zu Beginn des Evaluierungsprozesses findet die Prüfung des Schutzprofils statt. Danach folgt die Evaluierung der Sicherheitsvorgaben, die von der Zertifizierungsstelle erfolgreich abgenommen werden muss, bevor die eigentliche Evaluierung des EVG stattfindet. Während der Evaluation wird ein Evaluationsbericht von der Evaluationsstelle erstellt und die Zertifizierungsstelle überprüft die einheitliche Vorgehensweise auf Basis einer Evaluationsmethodologie. Wird der Evaluationsbericht erfolgreich abgenommen, endet die Evaluierung. Im Falle einer erfolgreichen Evaluation erstellt dann die Zertifizierungsstelle einen Zertifizierungsreport, der letztendlich zum Zertifikat führt und veröffentlicht ihn, falls gewünscht.

Eine Evaluierung auf Basis von CC ist natürlich auch mit **finanziellen Kosten** verbunden. Laut Corsec Security [28] gilt es dabei vier Faktoren zu berücksichtigen, um eine Kostenanalyse aufstellen zu können:

1. Die Kosten eines Testlabors
2. Den Änderungsaufwand und die damit verbundenen Kosten, ein Produkt den gestellten Anforderungen entsprechen zu lassen
3. Die Aufbereitung von Vertrauenswürdigkeitsdokumenten in für die Evaluierung notwendige Teilpakete
4. Die Gebühren der Offiziellen Zertifizierungsstellen

"… Feedback from the labs shows that testing for Evaluation Assurance Level **(EAL) 2** — the minimum level of security, which includes products such as firewalls, intrusion-detection systems, routers and switches — **costs $100,000 to $170,000** and takes four to six months. The highest level of security — **EAL 4**, which includes operating systems that support peer-to-peer communications — **costs $300,000 to $750,000** and takes one year to two years. " [25]

Das National Institute of Standards and Technology (NIST) hat den Schritt gewagt, ein Tool zur Vorbereitung und Unterstützung des Evaluationsprozesses produzieren zu lassen. Die CC Toolbox ist ein Open Source Projekt und daher kostenlos und frei verfügbar. Die **CC Toolbox** ist vollständig in Java implementiert und daher plattformunabhängig einsetzbar.

Das Ergebnis des Einsatzes der CC Toolbox in dieser Diplomarbeit ist ein selbst erstelltes standardisiertes Protection Profile für den zukünftigen Siemens internen Gebrauch, das **Radio Commander PP**. Es soll allgemeingültig sein für eine Vielzahl von Siemens Systemen und nur noch jeweils angepasst werden müssen. Das evaluierte IT-Produkt heißt Radio Commander und unterstützt die Steuerung von Mobilfunkantennen. Mit dem PP und dieser Diplomarbeit soll die Einführung von CC bei Siemens unterstützt werden. Das Schutzprofil kennzeichnet dabei die Sicherheitsanforderungen an ein IT-Gesamtsystem, welches aus Arbeitsplatzrechnern, Servern, Hosts und den sie verbindenden Netzkomponenten und der zum Betrieb der Anwendungen notwendigen Software bestehen kann.

Von anderen Schutzprofilen unterscheidet sich das Radio Commander PP dadurch, dass es Sicherheitsanforderungen für die Betrachtung von Gesamtsystemen und nicht für einzelne Komponenten formuliert; neben einer rollenbasierten Zugriffskontrolle eine benutzerbestimmte Zugriffskontrolle unter der Voraussetzung vertrauenswürdige Dateneigentümer toleriert; Anforderungen und Ergebnisse bezüglich der IT-Sicherheit berücksichtigt, die von den Erfahrung bisheriger Evaluierungen von IT-Systemen im Rahmen von Siemens basieren. Das vorliegende Radio Commander PP genügt der Vertrauenswürdigkeitsstufe EAL-4.

Das vollständige Radio Commander PP liegt im Anhang bei und stellt den praktischen Teil dieser Diplomarbeit dar.

Die Zukunft der CC Toolbox hängt also unweigerlich mit der **Zukunft von CC** zusammen. Damit CC noch mehr Einsatz finden wird, sind die an der Erstellung von CC beteiligten Institutionen zurzeit mit der Entwicklung der neuen Version 3.0 beschäftigt. Doch nur wenn die CC Toolbox bei einer neuen CC Version auch weiterentwickelt und angepasst wird, hat

sie Chancen weiterhin Verwendung zu finden. Nach Rücksprache mit Dr. Mackenbrock vom BSI ist bisher für die Mitte des Jahres 2005 kommende CC Version 3.0 weder die Weiterentwicklung der CC Toolbox noch die eines anderen Tools geplant.

Die neue Version wird voraussichtlich zwischen Mai und Juli 2005 veröffentlicht werden. Im Anschluss daran wird definitiv eine ISO Standardisierung für die neue Version von CC beantragt, so dass ungefähr ein Jahr später, 2006, die ISO Standardisierung Gültigkeit erlangen wird. Das Hauptaugenmerk bei der Überarbeitung der jetzigen CC Version liegt auf der Einbindung von praktischen Erkenntnissen. Dr. Mackenbrock verspricht aber, dass sich an den EAL-Stufen nichts ändern wird, ebenso wie am Zertifizierungsprozess an sich. Dennoch bezeichnet er die Änderungen als „mittel tief greifend", da die Struktur der Sicherheitsziele vollständig erneuert und der 2. Teil der CC auch komplett überarbeitet werden wird.

Trotz der neuen CC Version 3.0 scheuen noch viele Hersteller eine CC-Zertifizierung, da „Aufwand und Kosten mit der Prüftiefe steigen … Aus diesem Grund will das BSI die selektive Tiefenprüfung sicherheitsspezifischer Komponenten mit einer flächendeckenden Verbreitung von Sicherheitsprüfungen (wenn auch auf niedrigem Niveau) ergänzen. Die Schwelle zum Einstieg in CC-Evaluierungen muss also erniedrigt werden, das heißt das deutsche Interesse besteht darin, EAL1-Evaluierungen zu erleichtern und zu fördern." [24)]

Die kommenden Jahre werden zeigen, dass sich CC als internationaler Standard etabliert hat.

FACHHOCHSCHULE WÜRZBURG SCHWEINFURT
FACHBEREICH INFORMATIK UND WIRTSCHAFTSINFORMATIK

ERKLÄRUNG ZUR DIPLOMARBEIT

Hiermit versichere ich, dass die vorgelegte Diplomarbeit selbständig verfasst und noch nicht anderweitig zu Prüfungszwecken vorgelegt wurde.
Alle benutzen Quellen und Hilfsmittel sind angegebene,, wörtliche und sinngemäße Zitate und wurden als solche gekennzeichnet.

Würzburg, den 22.02.2005 .....